[redacted]

SEMESTER NOTES

Irish Debbarma

Department of Mathematics
Indian Institute of Science, Bangalore

December 2022

Contents

Part I.

Modular Forms

1. Lecture-1 (3rd January): Introduction

2. Lecture-2 (5th January, 2023):

3. Lecture-3 (10th January, 2023): Valence formula and Eisenstein series

3.1. Valence formula

Recall that $M_k(\Gamma_1)$ is the space of modular forms of weight k and level 1. It is also a vector space over $\mathbb{C}$.

Theorem 3.1.1.

$$\dim M_k(\Gamma_1) = \begin{cases} [k/12]+1 & k \not\equiv \pmod{12} \\ [k/12] & k \equiv \pmod{12} \end{cases}$$

Proposition 3.1.2.
Let $f \in M_k(\Gamma_1)$. Then,

$$\sum_{p \in \Gamma_1 \backslash \mathbb{H}} \frac{1}{n_p} \mathrm{ord}_p(f) + \mathrm{ord}_\infty(f) = \frac{k}{12}$$

Proof. Let $\epsilon > 0$ be "small enough". Remove ϵ-balls around $\infty, i, \omega, \omega+1$ in $\mathcal{F}_1$. ϵ is small enough so that the removed balls are disjoint. Truncate $\mathcal{F}_1$ at the line $y = \epsilon^{-1}$ and call the enclosed region D.
By Cauchy's theorem

$$\int_{\partial D} d(\log f(z)) = 0$$

This integral on the two vertical strips (just the straight lines not the semicircle part) is 0 since the contribution of left is same as right but orientation is different. On the segment joining $-1/2 + iY, 1/2 + iY$, the integral is $2\pi i \,\mathrm{ord}_\infty(f)$. Again,integral around each removed point in $\mathcal{F}_1$ is $\frac{1}{n_p}\mathrm{ord}_p(f)$. Next, divide the bottom arc into left and right parts and observe that

$$d(\log f(S \cdot z)) = d(\log f(z)) + k\frac{dz}{z}$$

$$\int_C d(\log f(z)) = \frac{k\pi i}{6}$$

□

Corollary 3.1.3.

$$\dim M_k(\Gamma_1) = \begin{cases} 0 & k < 0 \\ 0 & k \text{ is odd} \\ 1 & k = 0 \\ \begin{cases} [k/12]+1 & k \not\equiv \pmod{12} \\ [k/12] & k \equiv \pmod{12} \end{cases} \end{cases}$$

Proof.

- If $k < 0$, then f has poles but is holomorphic.
- If $k = 0$, then f is the constant function.
- We have seen
- For $m = [k/12] + 1$ let $f_1, \ldots, f_{m+1} \in M_k(\Gamma_1)$. Let $P_1, \ldots, P_m$ be any points on $\mathcal{F}_1$ not equal to $i, \omega, \omega + 1$ and consider $(f_i(P_j))_{i\in[m+1],j\in[m]}$.
  There exists a linear combination $f = \sum_{i=1}^{m+1} c_i f_i$ not all c_i being zero, such that $f(P_j) = 0$ for $1 \leq j \leq m$.
  From the previous theorem we get $f \equiv 0$ and this implies $\{f_i\}$ is linearly independent and thus $\dim_{\mathbb{C}} M_k(\Gamma_1) \leq m$.
  For $k \equiv 2 \pmod{12}$, the relation in previous theorem holds only if there is atleast a simple zero at $p = i$ and atleast a double zero at $p = \omega$. This gives

$$\frac{k}{12} - \frac{7}{6} = m - 1$$

  Repeat the argument above.

□

A slight notation. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we set $f|_\gamma(z) = (cz + d)^{-k} f(\gamma \cdot z)$.
Thus, $1|_\gamma(z) = (cz + d)^{-k}$. If $1|_\gamma(z) = 1 \Rightarrow c = 0$. Conversely, if $c = 0$, then $d^{-k} = 1$. So, $1|_\gamma(z) = 1 \Leftrightarrow c = 0$.
$\Gamma_\infty = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \right\} = \mathrm{stab}(\infty)$

3.2. Eisenstein series

Definition 3.2.1.
The Eisenstein series $E_k(z)$ is defined to be

$$E_k(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_1} 1|_\gamma(z)$$

Proposition 3.2.2.

$$E_k(z) = \frac{1}{2} \sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\},\gcd(c,d)=1} \frac{1}{(cz+d)^k}$$

Proof. □

Proposition 3.2.3.

$$\sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\},\gcd(c,d)=1} \frac{1}{(cz+d)^k}$$

converges absolutely for $k > 2$

Proof. □

Theorem 3.2.4.
$E_k(z) \in M_k(\Gamma_1)$ for $k > 2$.

Proof. □

Proposition 3.2.5.
$E_k(z) \not\equiv 0$ for $k > 2$, even.

Proof. Observe that

$$\frac{1}{(cz+d)^k} \to 0, \Im(z) \to \infty, c \neq 0$$

and if $c = 0$, then $c = \pm 1$. Hence, $E_k(z) = 1+$ bounded term as $\Im(z) \to \infty$. This implies $E_k(z) \not\equiv 0$ and

$$E_k(z) = 1 + \sum_{n=1}^{\infty} a_n e^{2\pi i z}$$

□

Another way of looking at Eisenstein series is a function on a lattice.
Consider $G_k(z) = G_k(\mathbb{Z}z + \mathbb{Z}) = \frac{1}{2}\sum'_{(c,d)\in\mathbb{Z}^2} \frac{1}{(cz+d)^k}$

Proposition 3.2.6.
$G_k(z)$ converges absolutely for $k > 2$.

Proposition 3.2.7.
$G_k(z) = \zeta(k)E_k(z)$

Proposition 3.2.8.
$\mathbb{G}_k(z) = \frac{(k-1)!}{(2\pi i)^k} G_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$ for $k > 2$, even.

4. Lecture-4 (12th January, 2023): Eisenstein series

4.1. Eisenstein series contd..

Recall that

$$M_*(\Gamma_1) = \bigoplus_{k\in\mathbb{Z}} M_k(\Gamma_1)$$

is a graded ring.

Proposition 4.1.1.
The graded ring $M_*(\Gamma_1)$ is freely generated by E_4, E_6. This means that the map

$$\begin{aligned} f : C[X,Y] &\to M_*(\Gamma_1) \\ X &\mapsto E_4 \\ Y &\mapsto E_6 \end{aligned}$$

is an isomorphism of graded rings. Here, $\deg X = 4, \deg Y = 6$.

Proof. We want to show that E_4 and E_6 are algebraically independent. We start by showing that E_4^3 and E_6^2 are linearly independent over $\mathbb{C}$. Suppose $E_6(z)^2 = \lambda E_4(z)^3$. Consider $f(z) = E_6(z)/E_4(z)$. Now observe that $f(z)^2 = \lambda E_4(z)$. This means that f^2 is holomorphic and thus f is also holomorphic. But f is weakly modular of weight 2 which is a contradiction. So, our claim is proven.

Claim: Let f_1, f_2 be two nonzero modular forms of same weight. If f_1, f_2 are linearly independent, then they are algebraically independent as well.

Let $P(t_1, t_2) \in \mathbb{C}[t_1, t_2]\backslash\{0\}$ be such that $P(f_1, f_2) = 0$. Let $P_d(t_1, t_2)$ be the d degree parts of P. Using the fact that modular forms of different weights are linearly independent, we get that $P_d(f_1, f_2) = 0 \ \forall \ d \geq 0$. If $p_d(t_1/t_2) = P_d(t_1, t_2)/t_2^d$, then $p_d(f_1/f_2) = 0$. But this means that f_1/f_2 is a constant. But, f_1, f_2 are linearly independent which implies that they are algebraically independent as well.

All of this implies that E_4, E_6 are algebraically independent. Using □

Corollary 4.1.2.

$$\dim_{\mathbb{C}} M_k(\Gamma_1) = \begin{cases} [k/12]+1 & k \not\equiv \pmod{12} \\ [k/12] & k \equiv \pmod{12} \end{cases}$$

4.1.1. Fourier expansions of $E_k(z)$

Proposition 4.1.3.

$$\mathbb{G}_k(z) = \frac{(k-1)!}{(2\pi i)^k} G_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

for $k > 2$, even and B_k are Bernoulli numbers.

Proof. Use

$$\frac{\pi}{\tan \pi z} = \sum_{n \in \mathbb{Z}} \frac{1}{z+n} = \lim_{M,N \to \infty, N-M < \infty} \sum_{-M}^{N} \frac{1}{z+n}$$

and

$$\frac{\pi}{\tan \pi z} = \frac{\pi \cos \pi z}{\sin \pi z} = \pi i \frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}} = -\pi i \frac{1+q}{1-q} = -2\pi i \left(\frac{1}{2} + \sum_{r=1}^{\infty} q^r \right)$$

This leads to the equality

$$\sum_{n \in \mathbb{Z}} \frac{1}{z+n} = -2\pi i \left(\frac{1}{2} + \sum_{r=1}^{\infty} q^r \right)$$

Differentiate both sides of equality $k-1$ times and divide by $(k-1)!$ to get

$$\sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{r=1}^{\infty} r^{k-1} q^r$$

Next, if we look at

$$\begin{aligned} G_k(z) &= \frac{1}{2} {\sum}' \frac{1}{(mz+n)^k} \\ &= \frac{1}{2} \sum_{n \in \mathbb{Z}, n \neq 0} \frac{1}{n^k} + \frac{1}{2} \sum_{(m,n) \in \mathbb{Z}^2, m \neq 0} \frac{1}{(mz+n)^k} \\ &= \zeta(k) + \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} \\ &= \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} r^{k-1} q^{mr} \\ &= \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sum_{r=1}^{\infty} \sigma_{k-1}(n) q^n \end{aligned}$$

The expression of $\mathbb{G}_k(z)$ is trivial after noting

$$\frac{(k-1)!}{(2\pi i)^k}\zeta(k) = B_k$$

□

Remark 4.1.4.
1. $\mathbb{G}_4(z) = \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + \cdots$
2. $\mathbb{G}_6(z) = -\frac{1}{504} + q + 33q^2 + 244q^3 + \cdots$
3. $\mathbb{G}_8(z) = \frac{1}{480} + q + 129q^2 + 2188q^3 + \cdots$

Proposition 4.1.5.

$$\sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m) = \frac{\sigma_7(n) - \sigma_3(n)}{120}$$

Proof. □

4.1.2. Weight 2 Eisenstein series

Definition 4.1.6.

$$\begin{aligned}\mathbb{G}_2(z) &= -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n)q^n \\ &= -\frac{1}{24} + q + 3q^2 + 4q^3 + 7q^4 + \cdots\end{aligned}$$

This converges rapidly on $\mathbb{H}$ and defines a holomorphic function.

Proposition 4.1.7.

$$G_2(z) = -4\pi^2\mathbb{G}_2(z)$$

Proof. Since we know that

$$G_2(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^2}$$

does not converge absolutely, we define

$$G_2(z) = \frac{1}{2}\sum_{n\in\mathbb{Z},n\neq 0} \frac{1}{n^2} + \frac{1}{2}\sum_{m\neq 0}\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2}$$

This sum converges absolutely and we can show that this satisfies the functional equation as required. □

Proposition 4.1.8.
For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$G_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 G_2(z) - \pi i c(cz+d)$$

G_2 is called a quasi modular form.

Introduce (due to Hecke):

$$G_{2,s}(z) = \frac{1}{2} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^2|mz+n|^{2s}}, \Re(s) > 0$$

4.2. Modular forms of higher level

Let $N \in \mathbb{Z}_{\geq 1}$

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z}) \mid ad - bc \equiv 1 \pmod{N} \right\}$$

Lemma 4.2.1.
The map

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}) &\to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \end{aligned}$$

is a surjective group homomorphism.

Proof. □

Definition 4.2.2.

$$\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$$

is called the principal congruence subgroup.

Definition 4.2.3.
A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if there exists N such

that $\Gamma(N) \subseteq \Gamma$.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z}) \mid c \equiv d \equiv 1 \pmod{N} \right\}$$

5. Lecture-5 (17th January, 2023): Congruence subgroups and $\triangle$ function

5.1. $\triangle$ function

Consider

$$\Delta(z) = \frac{1}{1729}(E_4^3(z) - E_6^2(z)) = q + q^2() + \cdots$$

Clearly, $\Delta(z)$ is a normalised cusp form of weight 12 and level 1.

Theorem 5.1.1.

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}, q = e^{2\pi iz}$$

Proposition 5.1.2.
$\Delta(z)$ has no zero in $\mathbb{H}$.

Proof. From the valence formula we have

$$\sum_{p\in\mathbb{H}} \frac{1}{n_p}\text{ord}_p(\Delta(z)) + \text{ord}_\infty(\Delta(z)) = k/12 = 1$$

Moreover, $\text{ord}_\infty(\Delta(z)) = 1$. Hence, we can conclude that $\text{ord}_p(\Delta(z)) = 0 \; \forall \; p \in \mathbb{H}$. □

Application: We use $\Delta(z)$ to write any modular form as a polynomial in E_4, E_6.

Take $f(z) \in M_k(\Gamma_1)$ with $4a + 6b, k \geq 4, a, b \geq 0$. The Fourier expansion of $f(z)$ can we written as

$$f(z) = a_0 + a_1 q + \cdots$$

Clearly, $f(z) - a_0 E_4^a(z)E_6^b(z) \in M_k(\Gamma_1) \subseteq S_k(\Gamma_1)$.
Next,

$$h(z) = \frac{f(z) - a_0 E_4^a(z)E_6^b(z)}{\Delta(z)} \in M_{k-12}(\Gamma_1)$$

Recursively, we can now find expression for $f(z)$.

Proposition 5.1.3.

$$j(z) = \frac{E_4^3}{\Delta(z)} = q^{-1} + \cdots$$

$$\begin{aligned} j : \bar{\mathbb{H}}/\Gamma_1 &\to \mathbb{P}^1(\mathbb{C}) \\ z &\mapsto j(z) \end{aligned}$$

is a bijection.

Proof. $E_4^3(z)$ and $\Delta(z)$ are linearly independent. For any $\lambda_1, \lambda_2 \in \mathbb{C}$ both not zero, $\lambda_1 E_4^3(z) + \lambda_2 \Delta(z)$ has an unique zero in $\bar{\mathbb{H}}/\Gamma_1$. □

Remark 5.1.4.
This j is called the j-invariant modular function. It attaches an elliptic curve in $\mathbb{P}^1(\mathbb{C})$ to any lattice in $\Lambda_z = \mathbb{Z}z + \mathbb{Z}$ and vice versa.

Next, the Fourier series of $\Delta(z)$ is of the form $\Delta(z) = \sum_{n\geq 1} \tau(n) q^n$ where $\tau(n)$ satisfies the following properties:

1. $\tau(pq) = \tau(p)\tau(q)$ if p, q are dinstinct primes.
2. $\tau(p^2) = \tau(p)^2 - p^{12-1}$.
3. $|\tau(p)| \leq 2p^{\frac{12-1}{2}}$.
4. $$\begin{aligned} \mathbb{G}_{12}(z) &= \Delta(z) + \frac{691}{156}\left(\frac{E_4^3(z)}{720} + \frac{E_6^2}{1008}\right) \\ \mathbb{G}_{12} &= -\frac{B_{12}}{24} + \sum_{n\geq 1} \sigma_{11}(n) q^n \\ &= \frac{691}{65520} + \sum_{n\geq 1} \sigma_{11}(n) q^n \\ \mathbb{G}_{12}(z) &\equiv \Delta(z) \pmod{691} \end{aligned}$$

   To conclude
   $$\tau(n) = \sigma_{11}(n) \pmod{691}$$
   (Related to the fact that $691 \mid \#\mathcal{C}\updownarrow(\mathbb{Q}(\gamma_{691}))$)

5.2. Congruence subgroup

Proposition 5.2.1.
Let $N = p_1^{a_1} \cdots p_r^{a_r}$ be the prime factorisation. Then,

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{i=1}^{r} \mathrm{SL}_2(\mathbb{Z}/p^{a_i}\mathbb{Z})$$

Lemma 5.2.2.

$$\#\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

Definition 5.2.3.
A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is called congruence subgroups if $\Gamma(N) \subseteq \Gamma$ for some $N \geq 1$.

Lemma 5.2.4.
A congruence subgroup has finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Remark 5.2.5.
There are non-congruence subgroups of finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Properties:

1. $\mathrm{PSL}_2(\mathbb{Z})$ is generated freely by an element of order 2 and an element of order 3.
2. S_7 is generated by an element of order 2 and an element of order 3. There is a surjection

$$\begin{aligned} \mathrm{PSL}_2(\mathbb{Z}) &\xrightarrow{\pi} S_7 \\ \pi^{-1}(\mathrm{Stab}_1) &\subseteq \mathrm{PSL}_2(\mathbb{Z}) \end{aligned}$$

3. $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is a simple group for $p \geq 5$.

Remark 5.2.6.
Γ is the smallest index subgroup that is non-congruence.

Definition 5.2.7.
A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight k and level Γ if

1. $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$
2. f is holomorphic at all cusps.

Cusps of $X(\Gamma)$ are just elements of $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$.

Proposition 5.2.8.

$$\text{orbit}(\infty) = \{\frac{a}{c} : p \mid c, p \nmid a\}, \text{orbit}(1) = \{\frac{a}{c} : p \nmid c\}$$

6. Lecture-6 (19th January, 2023): Congruence subgroups and enhanced elliptic curves

6.1. Congruence subgroups and modular forms of higher levels

Suppose p is a prime.

Proposition 6.1.1.

$$\#\left(\Gamma_0(p)\backslash^{\mathbb{P}^1(\mathbb{Q})}\right) = 2$$

Proof. □

Proposition 6.1.2.
Let Γ be a congruence subgroup, then $\Gamma\backslash^{\mathbb{P}^1(\mathbb{Q})}$ is finite. (called the cusps of level Γ).

Proof. □

Exercise 6.1.3.

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{j=0}^{p-1} \alpha_j \Gamma_0(p) \bigsqcup \alpha_\infty \Gamma_0(p)$$

where $\alpha_j = \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix}$ $0lej \leq p-1, \alpha_\infty = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

Notation: Let $f : \mathbb{H} \to \mathbb{C}$ be a function. Let $k \in \mathbb{Z}$ and $\gamma \in SL_2(\mathbb{R})$. We define

$$f|_{[\gamma]_k} : \mathbb{H} \to \mathbb{C}$$
$$\text{defined by } f|_{[\gamma]_k}(z) = (cz+d)^{-k} f(\gamma \cdot z)$$

With this notation: $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ if

- f is holomorphic on $\mathbb{H}$ and at ∞.
- $f|_{[\gamma]_k}(z) = f(z)\ \forall\ \gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Definition 6.1.4.
Let Γ be a congruence subgroup and $k \in \mathbb{Z}$. A modular form of weight k and level Γ is a function $f : \mathbb{H} \to \mathbb{C}$ such that

1. f is holomorphic on $\mathbb{H}$.
2. $f|_{[\gamma]_k} = f \ \forall \ \gamma \in \Gamma$.
3. f is holomorphic at all cusps.
   Note that $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$ for some $h \in \mathbb{Z}_{>0}$, and if $\Gamma(N) \subseteq \Gamma$ then $h \mid N$. Thus,
   $$f(z+h) = f(z)$$
   and f admits the Fourier expansion
   $$f(z) = \sum_{n \in \mathbb{Z}} a_n \exp(2\pi i n z/h)$$
   f is said to be holomorphic at ∞ if $a_n = 0 \ \forall \ n \leq -1$. Suppose $\alpha \in \mathbb{P}^1(\mathbb{Q})$ is a cusp, then there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \cdot \alpha = \infty$. f is holomorphic at α if $f|_{[\gamma]_k}$ is holomorphic at ∞.
4. $f|_{[\gamma]_k}$ is holomorphic at $\infty \ \forall \ \gamma \in \mathrm{SL}_2(\mathbb{Z})$

Example 6.1.5.
$\Gamma_1(p)$ has cusps $0, \infty$. We just need to check

- f is holomorphic at ∞.
- $f|_{[\gamma]_k}$ is holomorphic at ∞.

Notation:

$$M_k(\Gamma) = \text{ the space of modular forms of weight } k \text{ and level } \Gamma$$

Definition 6.1.6.
$f \in M_k(\Gamma)$ is said to be a cusp form if f vanishes at all cusps of level Γ, i.e., $f|_{[\gamma]_k}$ vanishes at $\infty \ \forall \ \gamma \in \mathrm{SL}_2(\mathbb{Z})$.

By $S_k(\Gamma)$ we denote the space of all cusp forms of weight k and level Γ.

$M(\Gamma) = \oplus_{k \in \mathbb{Z}} M_k(\Gamma)$ is the graded ring of modular forms of level Γ.

If $\Gamma_1 \subseteq \Gamma_2$ are two congruence subgroups, then $M_k(\Gamma_2) \subseteq M_k(\Gamma_1)$. This implies $M_k(\mathrm{SL}_2(\mathbb{Z})) \subseteq M_k(\Gamma)$ for any Γ.

Now, let Γ be a congruence subgroup. Define:

$$Y(\Gamma) = \Gamma\backslash\mathbb{H}$$
$$X(\Gamma) = \Gamma\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$$

These are called modular curves.

We saw that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ parametrises elliptic curves over $\mathbb{C}$ (upto isomorphism).

6.2. Enhanced elliptic curves

Let $N \in \mathbb{Z}_{\geq 1}$

Definition 6.2.1. 1. An enhanced elliptic curve of level $\Gamma_0(N)$ is a pair (E, C) where E is an elliptic curve and C is an order N cyclic subgroup of $E(\mathbb{C})$. Morphism between (E, C) and (E', C') is a homomorphism

$$\varphi : E \to E'$$

such that $\varphi(C) = C'$

2. An enhanced elliptic curve of level $\Gamma_1(N)$ is a pair (E, Q) such that E is an elliptic curve and Q is an order N point on $E(\mathbb{C})$.
Morphism between (E, Q) and (E', Q') is a homomorphism

$$\varphi : E \to E'$$

such that $\varphi(Q) = Q'$

3. An enhanced elliptic curve of level $\Gamma(N)$ is a triplet (E, Q_1, Q_2) such that E is an elliptic curve and Q_1, Q_2 are points of order N and

$$\langle Q_1, Q_2\rangle = E(\mathbb{C})[N] = \{x \in E(\mathbb{C}) \mid Nx = 0\}$$

Proposition 6.2.2. 1. $Y(\Gamma_0(N))$ parametrizes enhanced elliptic curves of level $\Gamma_0(N)$. The map $z \in \mathbb{H} \mapsto (\mathbb{C}/\Lambda_z, (1 + \Lambda_z)/\Lambda_z)$ gives a bijection between

$$Y(\Gamma_0(N)) \leftrightarrow \{\text{ isomorphism classes of enhanced elliptic curves of level } \Gamma_0(N)\}$$

2. $Y(\Gamma_1(N))$ parametrizes enhanced elliptic curves of level $\Gamma_0(N)$. The map $z \in \mathbb{H} \mapsto \left(\mathbb{C}/\Lambda_z, \frac{1}{N}\right)$ gives a bijection between

$$(\Gamma_1(N)) \leftrightarrow \{\text{ isomorphism classes of enhanced elliptic curves of level } \Gamma_1(N)\}$$

3. $Y(\Gamma(N))$ parametrizes enhanced elliptic curves of level $\Gamma_0(N)$. The map

$z \in \mathbb{H} \mapsto \left(\mathbb{C}/\Lambda_z, \frac{1}{N}, \frac{1}{N} \cdot z\right)$ gives a bijection between

$Y(\Gamma(N)) \leftrightarrow \{$ isomorphism classes of enhanced elliptic curves of level $\Gamma(N)\}$

Proof. □

Proposition 6.2.3.
The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is properly discontinuous, i.e., for $z_1, z_2 \in \mathbb{H}$ there exists neighbourhoods U_i of z_i such that if $\gamma \in U_1 \cap U_2 \neq 0$, then $\gamma \cdot z_1 = z_2$.

Proof. □

7. Lecture-7 (24th January, 2023): Riemann surfaces

Corollary 7.0.1.
$Y(\Gamma) = \Gamma\backslash\mathbb{H}$ with the quotient topology is Hausdorff.

Proof. □

Proposition 7.0.2.
$X(\Gamma)$ is compact.

Proof. □

7.1. Riemann surfaces

Definition 7.1.1.
A Riemann surface consists of the following data:

1. X is a topological space (Hausdorff + second countable).
2. (U_i, V_i, ϕ_i) with V_i open in X, U_i open ball in $\mathbb{C}$ and $\phi : U_i \to V_i$ a homeomorphisms such that whenever $V_i \cap V_j \neq \emptyset$ we have

$$\phi_j^{-1} \circ \phi_i : U_i \cap \phi_i^{-1}(V_i \cap V_j) \to U_j \cap \phi_j^{-1}(V_i \cap V_j)$$

to be homeomorphisms.

GOAL: To make $X(\Gamma)$ a Riemann surface. That is we want to construct charts on $X(\Gamma)$.

Definition 7.1.2.
A point $P \in Y(\Gamma)$ is called an elliptic point if for any lift z of P in $\mathbb{H}$, we have $\mathrm{Stab}_\Gamma(z)/\left(\mathrm{Stab}_\Gamma(z) \cap \{\pm I_2\}\right)$ is nontrivial. That is to say $\mathrm{Stab}_{\bar{\Gamma}}(z)$ is nontrivial, where $\bar{\Gamma}$ is the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.

P is an elliptic point in $Y(\Gamma)$ only if it lifts to a point equivalent to $i = \exp(2\pi i/4)$ or $\omega = 2\pi i/6$. If P is an elliptic point, then $\mathrm{Stab}_{\bar{\Gamma}}(z)$ has order 2 or 3.

7.1.1. Local charts on $Y(\Gamma)$

1. $P \in Y(\Gamma)$ is not an elliptic point.

   Let $z \in \mathbb{H}$ be a lift of P and U_1, U_2 be neighbourhoods of z. Put $U = U_1 \cup U_2$. If $\gamma U \cap U \neq \emptyset$, then the image set of Y in $\bar{\Gamma}$ is identity.

   $$\pi : \mathbb{H} \to Y(\Gamma)$$

   Put $\gamma = \pi(U)$. Then, $\pi|_U : U \to V$ is a homeomorphism.

2. Let $P \in Y(\Gamma)$ be an elliptic point. Let $z \in \mathbb{H}$ such that $\pi(z) = P$. Same as previous case get U_1, U_2 and define U as the the union of the two.
   Now, if $\gamma U \cap U \neq \emptyset$ then $\gamma \in \mathrm{Stab}_{\bar{\Gamma}}(z)$.
   Set $V = \pi(U)$. Notice that here $\pi|_U : U \to V$ need not be a homeomorphism. We instead have

   $$\begin{array}{ccc} U & \longrightarrow & U' = U/\mathrm{Stab}_{\bar{\Gamma}}(z) \\ {\scriptstyle \pi|_U}\downarrow & \swarrow_{\simeq} & \\ V & & \end{array}$$

3. We next want to extend this to cusps of $X(\Gamma)$.
   For $\mathrm{SL}_2(\mathbb{Z})$ we have already seen a local chart $z \mapsto \exp(2\pi i z)$. In general, take any cusp P of $X(\Gamma)$. Take $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma P = \infty$. Use the local charts at ∞.

Hence, $X(\Gamma)$ is a compact Riemann surface.

Next, we wish to compute genus of $X(\Gamma)$.
Genus $\mathfrak{g}$ of $X(\Gamma)$ is an integer such that

$$H^1(X(\Gamma), \mathbb{Z}) \cong \mathbb{Z}^{2g}$$
$$H_1(X(\Gamma), \mathbb{Z}) \cong \mathbb{Z}^{2g}$$

8. Lecture-8 (2nd February, 2023):

Part II.

Elliptic Curves

9. Lecture-1 (3rd January): Introduction

10. Lecture-2 (5th January, 2023): Affine varieties

10.1. Affine Varieties

Suppose k is a perfect field (every extension is separable).
Let $G(\bar{k}/k)$ be the Galois group of the extension. It can also be viewed as $\varprojlim_{L/K \text{Galois, } L \text{ finite}} \mathrm{Gal}(L/K)$.

11. Lecture-3 (10 January, 2023): Projective varieties

11.1. Projective varieties

Definition 11.1.1.
A Projective n-space over k denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\bar{K})$ is the set $\mathbb{A}^{n+1}\backslash\{(0,\ldots,0)\}/\sim$ with

$$(x_0,\ldots,x_n)\sim(y_0,\ldots,y_n)$$

iff $\exists\lambda\in\bar{k}^\times$ such that $(y_0,\ldots,y_n)=(\lambda x_0,\ldots,\lambda x_n)$
The equivalence class $(x_0,\ldots,x_{n+1})$ is denoted by $[x_0,\ldots,x_n]$
The set of k-rational points of $\mathbb{P}^n$ is

$$\mathbb{P}^n=\{[x_0,\ldots,x_n]\mid x_i\in k\}$$

Caution: If $p=[x_0,\ldots,x_n]\in\mathbb{P}^n(k)$ and $x_i\neq 0$ for some i, then $x_j/x_i\in k\forall j$

Definition 11.1.2.
Let $p=[x_0,\ldots,x_n]\in\mathbb{P}^n(\bar{k})$. The minimal field of definition for p is the field

$$k(p)=k(x_0/x_i,\ldots,x_n/x_i) \text{ for any } i \text{ such that } x_i\neq 0$$

$k(p)^{\frac{x_i}{x_j}}=k(x_0/x_j,\ldots,x_n/x_j)$ is the same as $k(p)$ as $x_i/x_j\in k(p)$

For $\sigma\in G(\bar{k}/k)$ and $p=[x_0,\ldots,x_n]\in\mathbb{P}^n$, we have the following action

$$\sigma(p)=[\sigma(x_0),\ldots,\sigma(x_n)]$$

This action is well defined as

$$\sigma(\lambda p)=[\sigma(\lambda)\sigma(x_0),\ldots,\sigma(\lambda)\sigma(x_n)]\sim[\sigma(x_0),\ldots,\sigma(x_n)]$$

Definition 11.1.3.
A polynomial $f\in\bar{k}[X_0,\ldots,X_n]$ is homogenous of degree d if

$$f(\lambda x_0,\ldots,\lambda x_n)=\lambda^d f(x_0,\ldots,x_n)\forall\lambda\in\bar{k}$$

Definition 11.1.4.
An ideal $I \subseteq \bar{k}[X_0, \ldots, X_n]$ is called a homogenous ideal if it is generated by homogenous polynomial.

Definition 11.1.5.
Let $I \subseteq \bar{k}[X_0, \ldots, X_n]$ be a homogenous ideal. Then,

$$V(I) = \{p \in \mathbb{P}^n(\bar{k}) \mid f(p) = 0 \; \forall \; f \in I\}$$

Definition 11.1.6.

- A projective algebraic set is any set of the form $V(I)$ for some homogenous ideal I.
- If V is a projective algebraic set, the homogenous ideal of V, denoted by $I(V)$ is the ideal of $\bar{k}[X_0 \ldots, X_n]$ generated by $\{f \in \bar{k}[X_0 \ldots, X_n] \mid f \text{ is homogenous and } f(p) = 0 \; \forall \; p \in V\}$
- Such a V is defined over k, denoted by V/k if its ideal $I(V)$ can be generated by homogenous polynomials $k[X_0 \ldots, X_n]$.
- If V is defined over k, then the set of k-rational points of V is

$$V(k) = V \cap \mathbb{P}^n(k) = \{p \in V \mid \sigma(p) = p \; \forall \; \sigma \in G(\bar{k}/k)\}$$

Example 11.1.7.
A line in $\mathbb{P}^2$ is given by the equation $aX + bY + cZ = 0$ with $a, b, c \in \bar{k}$ and not all 0 simultaneously.
If $c \neq 0$, then such a line is defined over a field containing $a/c, b/c$.
More generally, a hyperplane in $\mathbb{P}^n$ is given by an equation $a_0X_0 + \cdots + a_nX_n = 0$ with all $a_i \neq 0$ simultaneously.

Example 11.1.8.
Let V be the projective algebraic set in $\mathbb{P}^2$ given by $X^2 + Y^2 = Z^2$.

$$\begin{aligned} \mathbb{P}^1 &\xrightarrow{\sim} V \\ [s, t] &\mapsto [s^2 - t^2 : 2st : s^2 + t^2] \end{aligned}$$

Remark 11.1.9.
For $p \in \mathbb{P}^n(\mathbb{Q})$ you can clear the denominators and then divide by common factor so that $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. So, $I = (f_1, \ldots, f_m)$ and finding a rational point of V_I is same as finding coprime integer solutions to $f_i's$.

Example 11.1.10.
$V \subseteq \mathbb{P}^2$ such that $X^2 + Y^2 = 3Z^2$ over $\mathbb{Q}$. To find $V(\mathbb{Q})$, we just need to find integers a, b, c such that $a^2 + b^2 = 3c^2$

Example 11.1.11.
$V : 3X^3 + 4Y^3 + 5Z^3 = 0$. $V(\mathbb{Q}) = \emptyset$ but for all prime p we have $V(\mathbb{Q}_p) \neq \emptyset$

Definition 11.1.12.
A projective algebraic set is called a projective variety if its homogenous ideal $I(V)$ is prime $\bar{k}[X_0, \ldots, X_n]$

Relation between affine and projective varieties:

For $0 \leq i \leq n$

$$\begin{aligned} \phi_i : \mathbb{A}^n &\to \mathbb{P}^n \\ (Y_1, \ldots, Y_n) &\mapsto [Y_1, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n] \end{aligned}$$

$\mathrm{Im}(\phi) = U_i = \{p \in \mathbb{P}^n \mid \ p = [x_0 : \ldots : x_n] \text{ with } x_i \neq 0\} = \mathbb{P}^n \backslash H_i$.
This process can also be reversed by the following map :

$$\begin{aligned} \phi_i^{-1} : U_i &\to \mathbb{A}^n \\ [x_0 : \ldots : x_n) &\mapsto [x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i] \end{aligned}$$

Let V be a projective algebraic set with homogenous ideal $I(V) \subseteq \bar{k}[X_0, \ldots, X_n]$. Then,

$$V \cap \mathbb{A}^n = \phi_i^{-1}(V \cap U_i) \text{ for fixed } i$$

is an affine algebraic set with $I(V \cap \mathbb{A}^n) \subset \bar{k}[X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$

Definition 11.1.13.
Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set with ideal $I(V)$ and consider $V \subseteq \mathbb{P}^n$ and ϕ_i defined as before.
The projective closure of V is $\bar{V}$ is the projective algebraic set whose homogenous ideal $I(V)$ is generated by $\{f^* \mid f \in I(V)\}$.
Here, for $f \in k[X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ we define

$$f^*(X_0, \ldots, X_n) = X_i^d(f(X_0/X_i, \ldots, X_{i-1}/X_i, X_{i+1}/X_i, \ldots, X_n/X_i))$$

with $d = \deg(f)$.

Definition II.1.14.
Dehomogenization of $f(X_0, \ldots, X_n)$ with respect to i is $f(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n)$

Proposition II.1.15.
1. Let V be an affine variety. Then $\bar{V}$ is a projective variety and $V = \bar{V} \cap \mathbb{A}^n$.
2. Let V be a projective variety. Then, $V \cap \mathbb{A}^n$ is an affine variety and either $V \cap \mathbb{A}^n = \emptyset$ or $V = \overline{V \cap \mathbb{A}^n}$.
3. If an affine (resp. projective) variety V is defined over k, then $\bar{V}$ (resp. $V \cap \mathbb{A}^n$) is also defined over k.

Proof.
1.
2.
3.

□

Example II.1.16.
$V : Y^2 = X^3 + 17 \subseteq \mathbb{A}^2 \to \mathbb{P}^2$ with $(X, Y) \mapsto [X : Y : 1]$. Here, $\overline{V} : Y^2Z = X^3 + 17Z^3$ and $\overline{V} \backslash V = \{[0 : 1 : 0]\}$

12. Lecture-4 (12th January, 2023): Projective varieties and maps between varieties

12.1. Projective varieties contd..

Definition 12.1.1.

- Let Y/k be a projective variety and choose $\mathbb{A}^n \subseteq \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \emptyset$. The dimension of V is just dimension of $V \cap \mathbb{A}^n$.
- The function field of V, $\bar{k}(V) = \bar{k}(V \cap \mathbb{A}^n)$ is the function field for $V \cap \mathbb{A}^n$ over $\bar{k}$.
- Similarly, $k(V) = k(V \cap \mathbb{A}^n)$

$$\phi_i : \mathbb{A}^n \to \mathbb{P}^n \mathcal{I}(V \cap \mathbb{A}^n_i)$$
$$\phi_j : \mathbb{A}^n \to \mathbb{P}^n \mathcal{I}(V \cap \mathbb{A}^n_j)$$

For different ϕ_i we obtain $k(V)$s but they are canonically isomorphic to each other. This is because we can just switch x_i, x_j are dehomogenise accordingly.

Definition 12.1.2.
Let V be a projective variety and $p \in V$. Choose $\mathbb{A}^n \subseteq \mathbb{P}^n$ with $p \in \mathbb{A}^n$. Then, V is non-singular (or smooth) at p if $V \cap \mathbb{A}^n$ is non-singular at p.

The local ring of V at p, $\bar{k}[V]_p$ is just the local ring of $\bar{k}[V \cap \mathbb{A}^n]_p$

Remark 12.1.3.
Function field of a projective variety V is field of rational functions $f(X)/g(X)$ such that

1. f, g are homogenous of same degree.
2. $g \in \mathcal{I}(V)$.
3. $f_1/g_1 = f_2/g_2$ iff $f_1 g_2 - f_2 g_1 \in \mathcal{I}(V)$

Equivalently, take $f, g \in \bar{k}[X]/I(V)$ satisfying $1, 2$.

Here, X is just a short form for $(X_0, \ldots, X_n)$

12.2. Maps between varieties

Definition 12.2.1.
Let $V_1, V_2 \in \mathbb{P}^n$ be projective varieties. A rational map

$$\phi : V_1 \to V_2$$

$\phi = [f_0 : \cdots : f_n]$ where $f_i \in \bar{k}(V_1)$ such that $\forall p \in V_1$ at which f_i are defined, we have

$$\phi(p) = [f_0(p) : \cdots : f_n(p)]$$

If V_1, V_2 are defined over k, we have a Galois action. For $\sigma \in G(\bar{k}/k)$ we have

$$\sigma(\phi)(p) = [\sigma(f_0) : \cdots : \sigma(f_n)(p)]$$

We can check that $\sigma(\phi(p)) = \sigma(\phi)(\sigma(p))$.

Definition 12.2.2.
If $\exists \lambda \in \bar{k}^\times$ such that $\lambda f_i \in k(V_1)$, then ϕ is said to be defined over k.

Proposition 12.2.3.
ϕ is defined over k iff $\phi = \sigma(\phi)\ \forall\ \sigma \in G(\bar{k}/k)$.

Definition 12.2.4.
A rational map $\phi : V_1 \to V_2$ is said to be regular if there exists a function $g \in \bar{k}(V_1)$ such that

1. Each gf_i is regular at p.
2. There exists some i such that $(gf_i)(p) \neq 0$

If such a g exists, then we set

$$\phi(p) = [(gf_0)(p) : \cdots : (gf_n)(p)]$$

Definition 12.2.5.
A rational map is called a morphism if it is regular everywhere.

Remark 12.2.6.
Let $V_1, V_2 \in \mathbb{P}^n$ be projective varieties.
$\bar{k}(V_1) =$ quotient of homogenous polynomials in $\bar{k}[X]$ of same degree.
A rational map $\phi = [f_0, \ldots, f_n]$ can be multiplied by a homogenous polynomial to clear denominators and get $\phi = [\phi_0, \ldots, \phi_n]$ such that

1. $\phi_i \in \bar{k}[X]$ homogenous polynomials not all in $\mathcal{I}(V_1)$ and have same degree.
2. For all $f \in \mathcal{I}(V_2)$ we have $f(\phi_0(X), \ldots, \phi_n(X)) \in \mathcal{I}(V_1)$.

Definition 12.2.7.
A rational map $\phi = [\phi_0, \ldots, \phi_n] : V_1 \to V_2$ as above is regular at $p \in V_1$ if there exists homogenous polynomials $\psi_0, \ldots, \psi_n \in \bar{k}[X]$ such that

1. ψ_is have the same degree
2. $\phi_i\psi_j \equiv \phi_j\psi_j \pmod{\mathcal{I}(V_1)}$ for all $0 \leq i, j \leq n$
3. $\psi_i(p) \neq 0$ for some i.

If this happens, we set

$$\phi(p) = [\psi_0(p), \ldots, \psi_n(p)]$$

Remark 12.2.8.
Let $\phi = [\phi_0, \ldots, \phi_n] : \mathbb{P}^m \to \mathbb{P}^n$ be a rational map. ϕ_is are homogenous polynomials having same degree. We can cancel common factors to assume $\gcd(\phi_0, \ldots, \phi_n) = 1$.

And, ϕ is regular at a point $p \in \mathbb{P}^n$ iff $\phi_i(p) \neq 0$ for some i.
So, ϕ is a morphism if ϕ_is have no common zeros in $\mathbb{P}^n$.

Definition 12.2.9.
Let V_1, V_2 be two projective varieties. We say that V_1, V_2 are isomorphic if there are morphisms

$$\phi : V_1 \to V_2, \psi : V_2 \to V_1$$

such that $\phi \circ \psi = \mathrm{id}_{V_2}, \psi \circ \phi = \mathrm{id}_{V_1}$.
V_1/k and V_2/k are isomorphic over k if both maps are defined over k.

Example 12.2.10.
$\mathrm{char}(k) \neq 2$, $V : X^2 + Y^2 = Z^2$.

$$\begin{aligned} \phi : V &\to \mathbb{P}^2 \\ [X : Y : Z] &\mapsto [X + Z : Y] \end{aligned}$$

ϕ is regular everywhere except $[1:0:1]$
Since $(X+Z)(X-Z) \equiv -Y^2 \equiv \pmod{\mathcal{I}(V)}$, we have $[X+Z:Y] = [X^2-Z^2 : Y(X-Z)] = [-Y^2 : Y(X-Z)] = [-Y : X-Z] = \psi$

$$\begin{aligned} \psi : \mathbb{P}^1 &\to V \\ [s:t] &\to [s^2-t^2 : 2st : s^2+t^2] \end{aligned}$$

$\psi \circ \phi$ and $\phi \circ \psi$ are both identity maps.

Example 12.2.11.

$$\begin{aligned} \phi : \mathbb{P}^2 &\to \mathbb{P}^2 \\ [X:Y:Z] &\mapsto [X^2 : YZ : Z^2] \end{aligned}$$

is regular everywhere but $[0:1:0]$ and this cannot be salvaged.

Example 12.2.12.
$V : Y^2Z = X^3 + X^2Z$

$$\begin{aligned} \psi : \mathbb{P}^1 &\to V \\ [s:t] &\mapsto [(s^2-t^2)t : (s^2-t^2)s : t^3] \\ \phi : V &\to \mathbb{P}^1 \\ [X:Y:Z] &\mapsto [X:Y] \end{aligned}$$

ϕ is not regular at $[0:0:1]$. $[0:0:1]$ is a singular point of V which implies ϕ cannot be extended. So $\phi \circ \psi$ and $\psi \circ \phi$ are identities when they are defined.

Example 12.2.13.
$V_1 : X^2 + Y^2 = Z^2, V_2 : X^2 + Y^2 = 3Z^2$. $V_1 \ncong V_2$ over $\mathbb{Q}$ but $V_1 \cong V_2$ over $\mathbb{Q}(\sqrt{3})$.

13. Lecture-5 (17th January, 2023): Algebraic curves

13.1. Curves

Definition 13.1.1.
A curve is a projective variety of dimension 1.

Example 13.1.2.
Vanishing set of an irreducible polynomial in $\mathbb{P}^2$.

Proposition 13.1.3.
Let C be a curve and $p \in C$ be a smooth (non-singular) point. Then, $\bar{k}[C]_p$ is a discrete valuation ring.

Proof. $p \in C$ smooth implies M_p/M_p^2 is one dimensional over $\bar{k}[C]_p/M_p = \bar{k}$. Now, Nakayama will give us M_p is a principal ideal.

Claim: $\bigcap_n M_p^n = 0$.

Proof. If $\alpha \in \bigcap_n M_p^n$, then $\alpha = a_1 t = a_2 t^2 = a_3 t^3 = \cdots$. This implies $a_1 = a_2 t = a_3 t^2 = \cdots$. But this gives us a chain

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$$

that must terminate at some point. This implies t is an unit which is a contradiction. Hence, we are done. □

□

Definition 13.1.4.
Let C be a curve and $p \in C$ a smooth point. The normalised valuation on $\bar{k}[C]_p$ is

$$\begin{aligned} \mathrm{ord}_p : \bar{k}[C]_p &\to \mathbb{N} \cup \{0, \infty\} \\ f &\mapsto \sup\{d \in \mathbb{Z} \mid f \in M_p^d\} \\ \mathrm{ord}_p(\frac{f}{g}) &= \mathrm{ord}_p(f) - \mathrm{ord}_p(g) \end{aligned}$$

Thus we can define

$$\mathrm{ord}_p : \bar{k}[C] \to \mathbb{Z} \cup \{\infty\}$$

Definition 13.1.5.
An uniformiser for C at p is any function $t \in \bar{k}(C)$ with $\mathrm{ord}_p(t) = 1$ that is the generator of M_p

Remark 13.1.6.
If C is defined over k, we can find a unit $t \in k(C)$.

Definition 13.1.7.
Let C be a curve and $p \in C$ a smooth point, $f \in \bar{k}(C)$, $\mathrm{ord}_p(f) =$ order of f at p.

1. If $\mathrm{ord}_p(f) > 0$, then f has a zero at p.
2. If $\mathrm{ord}_p(f) < 0$, then f has a pole at p.
3. If $\mathrm{ord}_p(f) \geq 0$, then f is regular at p.

Proposition 13.1.8.
Let C be a smooth curve and $0 \neq f \in \bar{k}(C)$. Then, there are only finitely many points in C at which f has a pole or 0. If f has no poles, then $f \in \bar{k}$.

Proof. A standard exercise in Riemann surfaces. □

Example 13.1.9.
Suppose $C_1 : Y^2 = X^3 + X, C_2 : Y^2 = X^3 + X^2$. C_1 is smooth everywhere but C_2 is smooth everywhere except $p = [0 : 0 : 1]$.

In $\bar{k}[C_1]_p$, $M_p = \langle X, Y \rangle$ and $X \in M_p^2$.

Proposition 13.1.10.
Let C/k be a curve and $p \in C$ be a smooth point, and $t \in k(C)$ an uniformiser at p. Then, $k(C)$ is a finite separable extension of $k(t)$.

Proof. $k(C)$ is a finite algebraic extension as it is finitely generated over k and has transcendence degree 0 over $k(t)$ as t is not algebraic over k (it is a local coordinate of C at p).

Now, take $x \in k(C)$ and let $\Phi(T, X) = \sum a_{ij} T^i X^j$ be the minimal polynomial at x over $k(t)$. Say $q = \mathrm{char}(k)$. If $\Phi(T, X)$ is not separable, then $\frac{\partial \Phi(T,X)}{\partial X} = 0$ as $\Phi(T, X)$ is irreducible.

$$\begin{aligned}\Phi(T, X) &= \Psi(T, X^p) \\ &= \sum_{k=0}^{q-1} \left(\sum_{i,j} b_{ijk} T^{iq} X^{iq} \right) T^k \\ &= \sum_{k=0}^{q-1} (\Phi_k(T, X))^q \, T^k \text{ since } k \text{ is perfect, every element is a } q\text{-th power}\end{aligned}$$

$$\sum_{k=0}^{q-1} (\Phi_k(t, x))^q \, t^k = 0$$

$$\mathrm{ord}_p(\Phi_k(t, x)^q t^k) \equiv k \pmod{q}$$

This implies that every term in the final sum has distinct order at p. And, hence

$$\Phi_0(t, x) = \Phi_1(t, x) = \cdots = \Phi_{q-1}(t, x) = 0$$

Atleast one of the Φ_is should have a nonzero power of X and $X - \deg \Phi_i < X - \deg \Phi$ and hence $\Phi_k(t, x) = 0$ which contradicts minimality of Φ. Hence, we are done. □

13.2. Morphism between curves

Proposition 13.2.1.
Let C be a curve, $V \subseteq \mathbb{P}^n$ be a variety, $p \in C$ a smooth point and

$$\phi : C \to V$$

a rational map. Then, ϕ is regular at p. In particular, if C is smooth, then ϕ is a morphism.

Proof. Suppose $\phi = [f_0 : \cdots : f_n]$ with $f_i \bar{k}(C)$ and $t \in \bar{k}(C)$ an uniformiser for C at p. Let

$$n = \min \mathrm{ord}_p f_i$$

Then, $\mathrm{ord}_p(t^{-n} f_i) \geq 0 \; \forall \; i$ and $\mathrm{ord}_p(t^{-n} f_j) = 0$ for some j. But then this means $t^{-n} f_i$ are regular at p, $t^{-n} f_j(p) \neq 0$ and thus ϕ is regular at p. □

Remark 13.2.2.
This proposition is not true if either $\dim(C) > 1$ or p is singular

1. $\phi : \mathbb{P}^n \to \mathbb{P}^n$ be $[X : Y : Z] \mapsto [X^2 : YZ : Z^2]$ is not regular at $p = [0 : 1 : 0]$.

2. Suppose $V : Y^2Z = X^3 + X^2Z$ and $V \to \mathbb{P}^1$ be given by $[X : Y : Z] \mapsto [Y : X]$ is not regular at $[0 : 0 : 1]$.

Example 13.2.3. 1. $V : X^2 + Y^2 = Z^2$

14. Lecture-6 (19th January, 2023):

15. Lecture-7 (24th January, 2023):

16. Lecture-8 (31st January, 2023):

17. Lecture-9 (2nd February, 2023):

Part III.

Basic Algebraic Geometry

18. Lecture-1 (5th January): Introduction

19. Lecture-2 (10 January, 2023): Ideals and Zariski topology

19.1. Ideals

For I, J ideals

$$I + J = \{x + y \mid x \in I, y \in J\}$$
$$IJ = \{\sum x_i y_i \mid x_i \in I, y_i \in J\}$$

- $IJ \subseteq I \cap J$.
- If $I + J = R$, then $I^2 + J^2 = R$. This is because, say $I^2 + J^2 \neq R$, then there is a maximal ideal m such that $I^2 + J^2 \subseteq \mathfrak{m}$. This means $I^2, J^2 \subseteq \mathfrak{m}$. But $\mathfrak{m}$ is prime ideal, therefore $I, J \subseteq \mathfrak{m} \Rightarrow I + J \subseteq \mathfrak{m}$ which is a contradiction. Thus, we are done.
- If $\mathfrak{p}$ is a prime ideal and $IJ \subseteq \mathfrak{p}$. Then, $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$. Suppose not, then there exists $x \in I \backslash \mathfrak{p}, y \in I \backslash \mathfrak{p}$. But then $xy \in IJ \subseteq \mathfrak{p}$.
- $\mathfrak{p} \supseteq I \cap J \Leftrightarrow IJ \subseteq \mathfrak{p}$.

19.2. Zariski topology

Definition 19.2.1.
- For an ideal I, let
$$V(I) = \{\mathfrak{p} \text{ prime ideal } \mid I \subseteq \mathfrak{p}\}$$
- $\mathrm{Spec}(R) = \{$ collection of all prime ideals of $R\}$

Definition 19.2.2 (Zariski Topology)**.**
It is the topology defined on $\mathrm{Spec}(R)$ such that the closed sets are $V(I)$.

Verification that this indeed is a topology.

1. $V(0) = \mathrm{Spec}(R), V(R) = \emptyset$.
2. $V(I) \cup V(J) = V(I \cap J) = V(IJ)$.
3. $\bigcap_{k \in k} V_k = V(\sum_{k \in K} I_k)$. This is because $\mathfrak{p} \supseteq I_k \Leftrightarrow \mathfrak{p} \supseteq \sum_{k \in K} I_k$

Let us now look at the open sets of this topology. The basis for the open sets is given by

$$D(f \in R) = \{ \text{ all prime ideals not containing } f\}$$

Clearly,

$$(V(I))^c = \bigcup_{f \in I} D(f)$$

and moreover, each $D(f)$ is open since $D(f) = (V(\langle f \rangle))^c$

Theorem 19.2.3.
$\mathrm{Spec}(R)$ is quasi-compact.

Proof. We wish to prove that every open cover has a finite subcover. This is equivalent to saying every cover by $D(f_i)$ has a finite subcover. Say

$$\mathrm{Spec}(R) = \bigcup_{i \in I} D(f_i)$$

Take J to be the ideal generated by $f_i's$. Either $J = R$ or $J \subseteq \mathfrak{m}$. Suppose $J \subseteq \mathfrak{m}$, then $f_i \in \mathfrak{m} \in \mathrm{Spec}(R) \Rightarrow \mathfrak{m} \notin D(f_i)\ \forall\ i \Rightarrow D(f_i)$ does not cover $\mathfrak{m}$. A contradiction. Therefore, $J = R$ and this implies $1 =$ some linear combination of f_i and notice that this sum is finite. So, just consider these finitely many $f_i's$ (say the indexing set is K). These cover J. Suppose that $\{D(f_k), k \in K\}$ do not cover $\mathrm{Spec}(R)$. Then, there is a prime ideal $\mathfrak{p} \notin \bigcup_{k \in K} D(f_k) \Rightarrow \mathfrak{p} \ni f_k\ \forall\ k \in K \Rightarrow R \subseteq \mathfrak{p} \Rightarrow\Leftarrow$. Hence, it covers all of $\mathrm{Spec}(R)$ as required.

Another proof:
Suppose $\mathrm{Spec}(R) = \bigcup_{j \in J} U_j = \bigcup_{j \in J} \mathrm{Spec}(R) \backslash \mathcal{V}(I_j) = \mathrm{Spec}(R) \backslash \bigcap_{j \in J} \mathcal{V}(I_j) = \mathrm{Spec}(R) \backslash \mathcal{V}(\sum_{j \in J} I_j)$. This is equivalent to saying that $\mathcal{V}(\sum_{j \in J} I_j) = \emptyset$. So, we conclude that $\sum_{j \in J} I_j = R \Rightarrow$ $\sum_{k \in K} a_k = 1$ for some finite set K. We claim that $\{U_k : k \in K\}$ covers $\mathrm{Spec}(R)$. This is because

$$\begin{aligned} \mathcal{V}(\sum_{k \in K} I_k) &= 0 \\ \Rightarrow \mathrm{Spec}(R) &= \mathrm{Spec}(R) \backslash \mathcal{V}(\sum_{k \in K} I_k) \\ &= \bigcup_{k \in K} \mathrm{Spec}(R) \backslash \mathcal{V}(I_k) \\ &= \bigcup_{k \in K} U_k \end{aligned}$$

This completes the proof. □

Proposition 19.2.4.
Each $D(f)$ is quasi-compact.

Proof. Suppose

$$D(f) = \bigcup D(g_i)$$

and let J be the ideal generated by $g_i's$. Take $\mathfrak{p} \supseteq J$. Then, each $g_i \in J \subseteq \mathfrak{p} \Rightarrow \mathfrak{p} \notin D(g_i) \Rightarrow \mathfrak{p} \notin D(f) \Rightarrow f \in \mathfrak{p} \Rightarrow f \in \bigcap_{\mathfrak{p} \supseteq J} \mathfrak{p}$. Before completing this proof, we need to understand this intersection much better. Refer to following content on nilpotent elements and come back.
Now, we know that $f \in \mathrm{rad}(J)$ which implies $\exists n$ such that $f^n \in J$. We get

$$f^n = \sum_{\text{finite}} r_i g_i$$

Finally, we claim that these $D(g_i)$s cover $D(f)$. □

Definition 19.2.5.
$x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$.

Remark 19.2.6.
Any nilpotent element ($x^n = 0$ for some n) is clearly in every prime ideal ($0 \in \mathfrak{p}$) and thus in the intersection of all prime ideals. This can be recorded as

$$\bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p} \supseteq \mathrm{Nil}(R)$$

Proposition 19.2.7.

$$\bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p} \subseteq \mathrm{Nil}(R)$$

Proof. Take an element $x \in R \backslash \mathrm{Nil}(R)$ (not nilpotent) and consider the set

$$\Sigma = \{I \trianglelefteq R \mid x^n \notin I \ \forall\ n > 0\}$$

Notice that Σ is a poset with respect to inclusion. And every chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ has an upper bound (union of all the ideals). Thus, we can apply Zorn's lemma to get a maximal element $\mathfrak{p}$ which we claim is prime. Indeed, if $ab \in \mathfrak{p}$ but $a \notin \mathfrak{p}, b \notin \mathfrak{p}$ then $\mathfrak{p} + \langle a \rangle, \mathfrak{p} + \langle b \rangle$ are ideals strictly containing $\mathfrak{p}$ contradicting maximality of $\mathfrak{p}$. Therefore, we can conclude that $x \notin \mathfrak{p} \Rightarrow x \notin \bigcap_{\mathfrak{p} \supseteq J} \mathfrak{p}$ or rather not nilpotent implies not in intersection and hence we have proved the required inclusion. □

$$\mathrm{Nil}(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p} = \bigcap_{\mathfrak{p} \subseteq \{0\}} \mathfrak{p}$$

$$\{x \mid x^n \in J\} = \mathrm{rad}(J) = \bigcap_{\mathfrak{p} \supseteq J} \mathfrak{p}$$

20. Lecture-3 (12th January): Zariski topology

20.1. Zariski topology contd..

Definition 20.1.1.
If $J = \mathrm{rad}(J)$, then J is called radical ideal.

Properties:

1. Every radical ideal is an intersection of prime ideals.
2. $\mathcal{V}(J) = \mathcal{V}(\mathrm{rad}(J))$
3. $\mathcal{V}(J) = \mathcal{V}(J')$ implies $\mathrm{rad}(J) = \mathrm{rad}(J')$

Suppose $S \subseteq R$ such that

- $1 \in S, 0 \notin S$
- If $x, y \in S \Rightarrow xy \in S$

Proposition 20.1.2.
Take an ideal maximal wrt not intersecting S. Then, it is prime.

Proof. Suppose $\mathfrak{m}$ is the ideal in question. Next, suppose $\mathfrak{m}$ is not prime which implies $\exists a, b \in R$ such that $ab \in \mathfrak{m}$ but $a, b \notin \mathfrak{m}$. Then, $\mathfrak{m} + \langle a \rangle \supsetneq \mathfrak{m}, \mathfrak{m} + \langle b \rangle \supsetneq \mathfrak{m}$. But, this means $(\mathfrak{m} + \langle a \rangle) \cap S \neq \emptyset \Rightarrow m + ra \in S$ for some $m \in \mathfrak{m}, r \in R$. Similarly, $n + sb \in S$ for some $n \in \mathfrak{m}, s \in R$. But, S is multiplicative therefore $(m + ra)(n + sb) \in S \Rightarrow mn + ran + msb + rsab \in S \Rightarrow ((\langle ab \rangle + \mathfrak{m}) = \mathfrak{m}) \cap S \neq \emptyset$. This is a contradiction. Hence, we are done. □

Proposition 20.1.3.
Say J is maximal wrt not being principal. Then, J is prime.

Proof. Suppose $\mathfrak{m}$ is the ideal in question. Next, suppose $\mathfrak{m}$ is not prime which implies $\exists a, b \in R$ such that $ab \in \mathfrak{m}$ but $a, b \notin \mathfrak{m}$. Next, we can consider the ideal $I = \mathfrak{m} + \langle a \rangle$.

By maximality of $\mathfrak{m}$, we have $I = \langle c \rangle$ for some $c \in R$. Now, consider $J = \{x \in R \mid xc \in \mathfrak{m}\}$. Clearly, $I \subseteq J$. Notice that $c = m + ar$ for some $m \in \mathfrak{m}, r \in R$.

$$\begin{aligned} bc &= b(m + ar) \\ &= bm + (ba)r \\ \Rightarrow bc &\in \mathfrak{m} \\ \Rightarrow b &\in J \end{aligned}$$

This means $b \in J \backslash \mathfrak{m}$. Therefore V is also principal and hence $V = \langle d \rangle$. Since $\mathfrak{m} \in I$, therefore $m = cr$ for some $r \in R$. But this means that $r \in V \Rightarrow r = r'd$ for some $r' \in R$. Hence, $m = cdr' \in \langle cd \rangle \Rightarrow \mathfrak{m} \subseteq \langle cd \rangle$. For the other direction, since $d \in V \Rightarrow cd \in U$. All of these tells us that $\mathfrak{m} = \langle cd \rangle$ a contradiction to our assumption. Therefore, $\mathfrak{m}$ must be prime. □

Proposition 20.1.4.
Say J is maximal wrt not being finitely generated. Then, J is prime.

Proof. Suppose $\mathfrak{m}$ is the ideal in question. Next, suppose $\mathfrak{m}$ is not prime which implies $\exists a, b \in R$ such that $ab \in \mathfrak{m}$ but $a, b \notin \mathfrak{m}$.

If we now look at $\mathfrak{m} + \langle a \rangle$, by our assumption, this ideal is finitely generated by say $u_1, \ldots, u_m$. □

Exercise 20.1.5. *Suppose J is maximal wrt not being generated by a cardinal number of generators. Then, J is prime.*

Definition 20.1.6.
A topological space X is said to be irreducible if it cannot be written as the union of proper closed subsets of X

20.2. Identify closed irreducible subsets of $\mathrm{Spec}(R)$

Proposition 20.2.1.
The sets $\mathcal{V}(\mathfrak{p})$ are exactly the irreducible components of $\mathrm{Spec}(R)$.

Lemma 20.2.2.
Let $I \subseteq R$ be a radical ideal. If $\mathcal{V}(I)$ is irreducible, then I is prime.

Proof. Suppose I is not prime. Then there exists a, b such that $ab \in I$ but $a \notin I$ and $b \notin I$. Consider a prime ideal $\mathfrak{p}$ that contains I, it will also contain ab and thus $\mathfrak{p}$ contains either a or b. This is summarised as

$$\mathcal{V}(I) = (\mathcal{V}(I) \cap \mathcal{V}(a)) \cup (\mathcal{V}(I) \cap \mathcal{V}(b))$$

Thus $\mathcal{V}(I)$ is union of closed sets. It remains to be shown that the sets are proper in order to conclude that $\mathcal{V}(I)$ is not irreducible. Since $\mathcal{V}(I) \cap \mathcal{V}(a) = \mathcal{V}(I + \langle a \rangle)$ and $a \notin I$ therefore $\mathcal{V}(I + \langle a \rangle)$ is a proper closed subset of I and same for b. This is a contradiction to our hypothesis. So, we are done. □

Lemma 20.2.3.
$\mathcal{V}(\mathfrak{p})$ is an irreducible closed subset for $\mathfrak{p}$ prime.

Proof. Suppose $\mathcal{V}(\mathfrak{p}) = V_1 \cup V_2$ with V_1, V_2 proper closed subsets of $V(\mathfrak{p})$. Then there exists ideals I, J such that $\mathcal{V}(\mathfrak{p}) = \mathcal{V}(I) \cup \mathcal{V}(J)$. Since $\mathfrak{p} \in \mathcal{V}(\mathfrak{p})$ this implies $\mathfrak{p} \in \mathcal{V}(I)$ or $\mathfrak{p} \in \mathcal{V}(J)$. Suppose $\mathfrak{p} \in \mathcal{V}(I)$, then $I \subseteq \mathfrak{p} \Rightarrow \mathcal{V}(\mathfrak{p}) \subseteq \mathcal{V}(I) \Rightarrow \mathcal{V}(\mathfrak{p}) = \mathcal{V}(I)$. This is a contradiction to our assumption and hence we are done. $\mathcal{V}(\mathfrak{p})$ is irreducible. □

Proposition 20.2.4.
Every irreducible closed subset of $\mathrm{Spec}(R)$ has an unique generic point.

Proof. Notice that any irreducible closed subset is of the form $\mathcal{V}(\mathfrak{p})$. Now, $\mathcal{V}(\mathfrak{p})$ is the closure of $\mathfrak{p}$. This is because $\mathrm{cl}(\mathfrak{p})$ is a closed set and hence of the form $\mathcal{V}(I)$ for some ideal I. Moreover $\mathfrak{p} \supseteq I$. The biggest ideal I such that $I \subseteq \mathfrak{p}$ is $\mathfrak{p}$ and this gives us what we want because $\mathcal{V}$ reverses inclusions. Therefore, $\mathrm{cl}(\mathfrak{p}) = \mathcal{V}(\mathfrak{p})$. And, such a generic point is unique for suppose $\mathcal{V}(\mathfrak{p}) = \mathcal{V}(\mathfrak{q})$ then clearly $\mathfrak{p} \subseteq \mathfrak{q}$ and $\mathfrak{q} \subseteq \mathfrak{p}$. So, we are done. □

To summarise, Zariski topology has the following properties:

1. $\mathrm{Spec}(R)$ is quasi-compact
2. $\mathrm{Spec}(R)$ has a basis of quasi-compact opens which is closed under intersection.
3. Every irreducible closed subset has a generic point.

Theorem 20.2.5 (Hochster)**.**
Any topological space with the 3 properties is the spectrum of some commutative ring.

Suppose X is spectral. Define a new space X^* with open sets as finite union of quasi-compact open sets in X. This new space is called the Hochster dual.

Theorem 20.2.6.
X^* is also spectral.

Proof. □

21. Lecture-4 (17th January, 2023): Noetherian spaces

21.1. Noetherian spaces

First, let us try to remember all the equivalent definitions of a ring being Noetherian.

Proposition 21.1.1.
The following are equivalent:

1. Every ideal is finitely generated.
2. Every ascending chain of ideals
$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$
stabilises.
3. Every non-empty family of ideals has a maximal element.

Nowhere do we use Zorn's lemma, so in some sense, these properties are essentially about some "finite-ness" property. Thus, Noetherian means strong finiteness in some sense.

Definition 21.1.2.

Definition 21.1.3.

Theorem 21.1.4.
A module M over R is Noetherian iff the module is finitely generated and finitely presented.

Proof. □

Proposition 21.1.5.
The direct sum of projective modules is projective.

Proposition 21.1.6.
The direct product of injective modules is injective.

A question we can ask is when is the direct sum of injective modules injective.

Proposition 21.1.7.
Direct sum of injective modules is injective iff the module is Noetherian.

22. Lecture-5 (19th January 2023):

Suppose A is a commutative ring and M an A-module.
Define $\mathrm{Sub}(M) =$ to be the set of all submodules of M. For any finite collection $m_1, \ldots, m_k \in M$, we next define

$$\mathbf{V}(m_1, \ldots, m_k) = \text{ collection of submodules containing } m_1, \ldots, m_k$$
$$\mathbf{D}(m_1, \ldots, m_k) = \mathrm{Sub}(M) \backslash \mathbf{V}(m_1, \ldots, m_k)$$

Using these $\mathbf{D}(m_1, \ldots, m_k)$'s as open sets (sub-basis of open sets), we generate a topology.

Proposition 22.0.1 (read this here)**.**
The above mentioned topology is the same as Zariski topology OR the space is spectral.

Remark 22.0.2.
The takeaway point being this is also another way to get a spectral space.

Exercise 22.0.3. *Suppose X is spectral, $Y \subseteq X$ be a quasi-compact open subset. Then, Y is spectral.*

22.1. Localisation

Definition 22.1.1.
A multiplicatively closed set S is one that has the following properties:

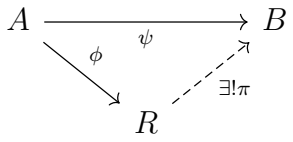
1. $1 \in S, 0 \notin S$.
2. $x, y \in S \Rightarrow xy \in S$.

Example 22.1.2.
1. Invertible elements of a ring.
2.

Objective: We wish to construct a new ring in which each $s \in S$ is invertible.

If S was the collection of invertible elements, then localisation is just A.

Our objective can be summed up as follows:



1. $\phi(s)$ is invertible in R for each $s \in S$
2. for any $\psi : A \to B$ such that each $\psi(s)$ is invertible, there is an unique map $\pi : R \to B$ that makes the diagram above commute.

Definition 22.1.3.
The localisation of A with respect to S, denoted by $S^{-1}A$ is the set of equivalence classes

$$\frac{a}{s} \quad , a \in A, s \in S$$

with

$$\frac{a}{s} \sim \frac{a'}{s'} \text{ if and only if } \exists\ t \in S \text{ such that } t(as' - sa') = 0$$

The ring addition and multiplication are the same as adding and multiplying fractions. Need to check it is well-defined!

Now, back to

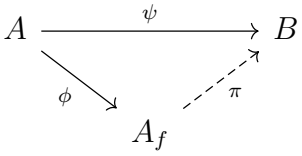
$$A_f = \{ \text{ localisation of } A \text{ at } f \}$$

What we want to do is we essentially want to turn f into an unit. Take S to be all powers of f. Then, $S^{-1}A = A_f$.

This can also be realised as

$$\frac{A[X]}{\langle fX - 1 \rangle}$$

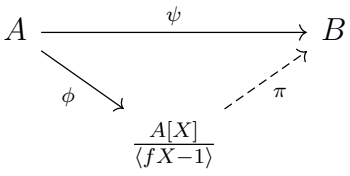
Now, the question is why are the two notions equivalent.



with

$$\pi\left(\frac{a}{f^k}\right) = \frac{\psi(a)}{\psi(f)^k}$$

And,



with $\pi(X) = \psi(f)^{-1}$

22.1.1. Prime ideals of A_f

Theorem 22.1.4.
The prime ideals of A_f are precisely $D(f)$ the set of primes not containing f.

Consider A_S and look at the ideals of A_S. They are precisely of the form

$$\left\{ \frac{x}{s} \mid \ x \in I \subseteq A, s \in S \right\}$$

There is a bijection between

$$\{ \text{ prime ideals of } A_S \} \leftrightarrow \{\text{prime ideals of } A \text{ not intersecting S}\}$$

23. Lecture-6 (24th January, 2023): Localisation of modules, exact sequences

23.1. Localisation contd..

Suppose M is an A-module. And $S \subseteq A$ be a multiplicative set. Then, the localisation

$$M_S = \{\text{equivalence classes of all elements of the form } \frac{m}{s}\}$$

with $\frac{m}{s} \sim \frac{m'}{s'}$ if there exists $t \in S$ such that $t(s'm - m's) = 0$. This can be made into a module by standard operations.

Lemma 23.1.1.
M_S is an A_S-module.

Proof. □

Some natural questions to ask are if $I \subseteq A$ is an ideal, whether

$$\left(\frac{A}{I}\right)_S \overset{?}{\cong} \frac{A_S}{I_S}$$

$$\text{More generally } \left(\frac{M}{M'}\right)_S \overset{?}{\cong} \frac{M_S}{M'_S}$$

We will need to introduce exact sequences to answer these questions.

23.2. Exact sequences

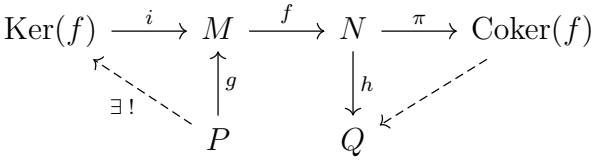
Suppose

$$f : M \to N$$

Then,

$$\ker(f) = \{m \in M : f(m) = 0\}$$
$$\text{Coker} = N/\text{Im}(f)$$

This can be captured in the following diagram :



Here,

$$M/\ker(f) \cong \mathrm{Im}(f)$$

is equivalent to saying $\mathrm{Coker}(i) = \ker(\pi)$. This leads to the definition

Definition 23.2.1.

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact at M if $\mathrm{Im}(f) = \ker(g)$.

Lemma 23.2.2. 1.

$$0 \to M' \xrightarrow{f} M$$

being exact means f is injective.

2.

$$M \xrightarrow{g} M'' \to 0$$

being exact means g is surjective.

Proof. □

Definition 23.2.3.
A short exact sequence is a sequence of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is exact everywhere.

Proposition 23.2.4.
If

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

is exact, then

$$0 \to M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S \to 0$$

is exact

Next, take $\mathfrak{p} \subseteq A$ be a prime ideal and $A \backslash \mathfrak{p}$ be the multiplicative set S. We denote M_S by $M_{\mathfrak{p}}$.

- If $M = 0$, then $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$. This implies $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$.
- If $M_{\mathfrak{m}} = 0 \; \forall \; \mathfrak{m} \Rightarrow M = 0$.
- If $M \xrightarrow{f} N$ is an isomorphism iff $M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}}$ is an isomorphism for all maximal ideals $\mathfrak{m}$.

Definition 23.2.5.
Suppose

$$M \xrightarrow{f} N$$

Then, f is a monomorphism means

$$T \underset{h}{\overset{g}{\rightrightarrows}} M \xrightarrow{f} N$$

such that $f \circ g = f \circ h \Rightarrow g = h$.

Epimorphism is the dual of this.

Remark 23.2.6.
For sets, these mean injection and surjection but monomorphism and epimorphism need not mean isomorphism in a random category.

24. Lecture-7 (31st January, 2023):

25. Lecture-8 (2nd February, 2023):

Part IV.

Algebraic Geometry I

26. Lecture-1 (9th January, 2023): Topological properties and Zariski Topology

26.1. Topological properties

Consider a topological space X.

Definition 26.1.1.
1. We say X is quasi-compact if every open cover of X admits a finite subcover.
2. If $f : X \to Y$ is continuous, we call f quasi-compact if $f^{-1}(V)$ is quasi-compact for all quasi-compact open $V \subseteq Y$.

Exercise 26.1.2. *Composition of quasi-compact maps is quasi-compact.*

Consider the two maps $f : X \to Y$ and $g : Y \to Z$. Next, look at the composition $g \circ f : X \to Z$. For all quasi-compact open $V \subseteq Z$, $(g \circ f)^{-1}(V) = f^{-1} \circ g^{-1}(V)$. Since g is quasi-compact and continuous, $g^{-1}(V)$ is also quasi-compact and open. Similarly, f is also quasi-compact and continuous, therefore $f^{-1}(g^{-1}(V))$ is also quasi-compact and we are done.

Lemma 26.1.3.
X quasi-compact and $Y \subseteq X$ is closed implies Y is quasi-compact.

Proof. Let $\{U_i\}_{i \in I}$ be an open cover of Y. Set $U = X - Y$. Since U_i is open in Y, we have $U_i = Y \cap V_i$ where V_i is open in X. Now we note that $\{V_i\}_{i \in I} \cup U$ covers X but X is quasi-compact and we obtain a finite subcover $\{V_i\}_{i \in J} \cup U$ where J is finite. The corresponding $U_i, i \in J$ must therefore cover Y and we are done. □

Proposition 26.1.4.
If X is quasi-compact and Hausdorff, then $E \subseteq X$ is quasi-compact iff E is closed.

Proof. $\Leftarrow$ direction is done.
$\Rightarrow$ direction is what we need to prove.
Take $x \in X \backslash E$. For each $y \in E$, due to Hausdorff-ness we have two disjoint open sets U_y and U_y containing x and y respectively. Do this for all $y \in E$. The collection

$\{U_y\}_{y\in E}$ covers E but it is quasi-compact thus we get a finite subcover $\{U_{y_i}\}_{i\in I}$ with I finite. Now, let

$$U = \bigcap_{i\in I} U_{y_i}$$

U is clearly open, contains x and is disjoint from E. Since x was chosen arbitrarily, $X\backslash E$ must be open. □

Lemma 26.1.5.
Any finite union of quasi-compact spaces is quasi-compact.

Proof. Suppose $X_i, i = 1, 2, \ldots, n$ are the spaces in question. We want to show that

$$X = \bigcup_{i=1}^{n} X_i$$

is also quasi-compact. Take any cover $\{U_i\}_{i\in I}$ be an open cover of X. Then for each $i = 1, 2, \ldots, n$ it is clear that $\{U_i\}_{i\in I}$ also covers X_i. Using quasi-compactness of X_i we can get a finite subcollection $\{U_{i_j} : j = 1, \ldots, n_i\}$. This can be done for all i. Now, consider $\bigcup_{i=1}^{n}\bigcup_{j=1}^{n_i} U_{i_j}$. This union covers X and is finite. So, we are done. □

Lemma 26.1.6.
Suppose $f : X \to Y$ is continuous, if X is quasi-compact then so is $f(X)$.

Proof. Let $\{U_i\}_{i\in I}$ be an open cover of $f(X)$. Now, $\{f^{-1}(U_i)\}_{i\in I}$ covers X and by continuity, each of them are open. Use quasi-compactness of X to get a finite subcover that covers X.

$$\begin{aligned} X &= \bigcup_{i=1}^{n} f^{-1}(U_i) \\ \because f(f^{-1}(U_i)) &\subseteq U_i \\ \therefore f(X) &\subseteq \bigcup_{i=1}^{n} U_i \end{aligned}$$

□

Suppose Σ is a poset. Σ satisfies acc if every ascending chain

$$x_1 \leq x_2 \leq \cdots$$

is stationary.

Lemma 26.1.7.
The following are equivalent:

1. Σ satisfies acc.

2. Every non-empty subset of Σ has maximal element.

Proof. $1 \Rightarrow 2$. Suppose $S \subseteq \Sigma$ has no maximal element.
Then choose $x_0 \in S$ non-maximal, then we can find a x_1 such that $x_0 \lneq x_1$. By induction we can construct an infinite chain $x_0 \lneq x_1 \lneq \cdots \neq x_i \lneq \cdots$ which does not terminate which is a contradiction to our hypothesis. Thus, S must have a maximal element.
$2 \Rightarrow 1$. Suppose $x_1 \leq x_2 \leq \cdots \leq x_i \leq$ is an infinite ascending chain, then $S = \{x_i \mid i \geq 1\}$ has no maximal element. □

Definition 26.1.8.
A topological space is called Noetherian if set of all closed subsets of X satisfies dcc.

Lemma 26.1.9.
X Noetherian implies X is quasi-compact.

Proof. Let $\mathcal{U} = \{U_i\}_{i \in I}$ be an open cover of X that does not have a finite subcover. Consider the collection $\mathcal{F}$ of union of finite number of elements of $\mathcal{U}$. Since being Noetherian is equivalent to saying any finite subset of open subsets has a maximal element, we know that $\mathcal{F}$ has a maximal element. Suppose that maximal element is $U_{i_1} \cup \ldots \cup U_{i_n}$. If this does not cover X, take an element x in the complement of the maximal element. Since $\mathcal{U}$ covers X, there is an $i \in I$ such that $x \in U_i$. Notice that now $U_{i_1} \cup \ldots \cup U_{i_n} \subseteq U_{i_1} \cup \ldots \cup U_{i_n} \cup U_i$ which contradicts the maximality. Thus, we are done. □

Remark 26.1.10.
The converse need not be true. Consider $[0, 1]$ covered by $[1/2^n, 1]$.

Lemma 26.1.11.
If $X_1, \ldots, X_n$ are Noetherian subspaces of X, then so is $X = X_1 \cup X_2 \cup \ldots \cup X_n$

Proof. Let Y_is be closed in X that forms the chain

$$X \supseteq Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \cdots$$

For each i, we get a chain of closed sets in X_i by intersecting with X_i. This gives us

$$X_i \supseteq Y_1 \cap X_i \supseteq Y_2 \cap X_i \supseteq Y_3 \cap X_i \supseteq \cdots$$

Since X_i is Noetherian, this chain terminates at say r_i. Now, take $r = \max_i r_i$. The original chain will terminate after this point. Suppose $y \in Y_i$ with $i \leq r$, there is an j such that $y \in X_j$. This means $y \in X_j \cap Y_i = X_j \cap Y_r$. Hence, $y \in Y_r$ and we are done. □

Definition 26.1.12.
Locally Noetherian means every point $x \in X$ has a neighbourhood U which is Noetherian wrt subspace topology.

Lemma 26.1.13.
Quasi-compact and locally Noetherian implies Noetherian.

Proof. Since X is locally Noetherian, for each $x \in X$ we have a nbd. U_x that is Noetherian. $\{U_x\}_{x\in X}$ is an open cover of X. Quasi-compactness gives us a finite subcover $\{U_{x_i}\}_{i=1}^{n}$, i.e.,

$$X = \bigcup_{i=1}^{n} U_{x_i}$$

X is Noetherian from previous lemma. □

Exercise 26.1.14. *Give an example of a ring R such that $\mathrm{Spec}(R)$ is Noetherian but R is not.*

Consider the ring $R = k[X_1, X_2, \ldots,]$ and the ideal $I = \langle X_1^2, X_2^2, \ldots, \rangle$. Now, look at $R' = R/I$. $\mathrm{Spec}(R')$ is a singleton.

Definition 26.1.15.
A topological space X is called irreducible if it cannot be written as finite union of proper closed subsets.

A closed subset $Y \subseteq X$ is called irreducible component of X if it is a maximal irreducible closed subset of X.

Lemma 26.1.16.
If X is Noetherian and $Y \subseteq X$ is a subspace, then Y is Noetherian.

Proof. Let Y_is be closed in Y that forms the chain

$$Y \supseteq Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \cdots$$

For each i, we have a closed set in X such that $Y_i = Y \cap X_i$. This gives us

$$Y \supseteq X_1 \cap Y \supseteq X_2 \cap Y \supseteq X_3 \cap Y \supseteq \cdots$$

□

Lemma 26.1.17.
Let X be Noetherian. Then, X has finitely many irreducible components.

Proof. More generally, we will show that every closed subset for X has finitely many irreducible components.

Suppose that this is false. Let Σ be the collection of closed subsets of X that does not satisfy our condition. Order this as follows: $A \leq B$ if $A \supseteq B$. If $\{C_i\}$ is a chain in Σ, then it must eventually stabilise since X is Noetherian. This C_α is an upper bound for this chain. Therefore, by Zorn's lemma, there is a maximal element Y. Since $Y \in \Sigma$, therefore it is not irreducible. Suppose $Y = Y_1 \cup Y_2$ with Y_1, Y_2 proper closed subsets of Y. $Y \leq Y_1, Y \leq Y_2$. Since $Y \in \Sigma$, Y is not a finite union of irreducible components. Hence, either Y_1 or Y_2 is not irreducible. If Y_1 is not irreducible but $Y_1 \in \Sigma$, since Y is maximal in Σ and $Y \leq Y_1$, therefore $Y = Y_1$ a contradiction that Y_1 is a proper subset of Y. Thus, Σ must be empty and the claim is proven. □

Lemma 26.1.18.
X is Noetherian implies there exists an unique expression $X = X_1 \cup \cdots \cup X_n$ where $X_i's$ are irreducible components of X.

Proof. Suppose

$$X = X_1 \cup \cdots \cup X_n = X_1' \cup \cdots \cup X_m'$$

Clearly $X_1' \subseteq X$, this means $X_1' = \bigcup_{i=1}^n X_1' \cap X_i$. Since X_1' is irreducible, there must be a i_1 such that $X_1' = X_{i_1} \cap X_1'$. Thus, $X_1' \subseteq X_{i_1}$. We can choose i_1 to be 1 to get $X_1' \subseteq X_1$. Similarly, $X_1 \subseteq X_{j_1}'$. Since $X_1' \subseteq X_{j_1}'$ and our assumption that $X_i \not\subseteq X_j$ for $i \neq j$ we conclude that $j_1 = 1$. Finally, we conclude that $X_1 = X_1'$. Let Z be the closure of $X - X_1$, then $Z = X_2 \cup \cdots \cup X_n = X_2' \cup \cdots \cup X_m'$. We can argue inductively and conclude that $X_i = X_i'$ and $n = m$. □

Lemma 26.1.19.
Suppose X is Noetherian and $X_1 \subseteq X$ an irreducible component. Then, X_1 contains a non-empty open set in X.

Proof. Consider $U = X \backslash X_2 \cup \cdots \cup X_n$. Clearly, U is non-empty and open. Moreover, $U \subseteq X_1$ and we are done. □

Definition 26.1.20.
Let X be a topological space. We say that X is a spectral space if the following holds:

1. X is quasi-compact.
2. X is T_0.
3. X has a basis of quasi-compact open sets.

4. Every irreducible closed subset of X has a generic point ($\exists x \in Y$ such that $\overline{\{x\}} = X$)

26.2. Zariski Topology

Let A be a commutative ring with identity and $X = \mathrm{Spec}(A)$.

Zariski topology is the unique topology such that a subset $Y \subseteq X$ is closed iff $Y = \mathcal{V}(I)$ for some ideal $I \trianglelefteq A$. Here,

$$\mathcal{V}(I) = \{\mathfrak{p} \in X \mid \mathfrak{p} \supseteq I\}$$

Theorem 26.2.1.
$\mathrm{Spec}(A)$ is always spectral.

Proof. 1. X is T_0
For all $f \neq 0$ in A, let $A_f = S^{-1}A$ be the localisation of A at f where $A_f = \{f^n \mid n \geq 0\}$. Next, let $V_f = X \backslash V(f) = \mathrm{Spec}(A_f)$. This forms a basis for the Zariski topology.
Now, let $\mathfrak{p}, \mathfrak{P}$ be two distinct primes.

- Suppose $\mathfrak{p} \not\subseteq \mathfrak{P}$.
  $Y = V(\mathfrak{p})$ is closed set and $\mathfrak{P} \notin V(\mathfrak{p})$. Take Y^c. Then $\mathfrak{P} \in Y^c$ and $\mathfrak{p} \notin Y^c$.
- If $\mathfrak{p} \subseteq \mathfrak{P}$
  Then consider $\mathcal{V}(\mathfrak{P})$. Clearly, $\mathfrak{p} \notin \mathcal{V}(\mathfrak{P})$. Take $U = \mathcal{V}(\mathfrak{P})^c$, then $\mathfrak{p} \in U$ but $\mathfrak{P} \notin U$.

2. X is quasi-compact.
Let $\{U_i\}$ be an open cover of X. WLOG, we can assume that $U_i = \mathrm{Spec}(A_{f_i}), f \neq 0$. Let I be the ideal generated by these f_is.
Case-1: Suppose that $I \neq A$. Then there exists a maximal ideal $\mathfrak{m} \supseteq I \Rightarrow \mathcal{V}(\mathfrak{m}) \subseteq \mathcal{V}(I) \Rightarrow X \backslash \mathcal{V}(\mathfrak{m}) \supseteq X \backslash \mathcal{V}(I) = X \backslash \bigcap_{i \in I} \mathcal{V}(f_i) = \bigcup U_i = X$ which is absurd. Hence, we conclude that $I = A$. Next,

$$1 = \sum_{i=1}^{n} a_i f_i \qquad \text{for some } a_i \in A$$
$$\Rightarrow \bigcup_{i=1}^{n} U_i = \bigcup_{i=1}^{n} X \backslash \mathcal{V}(f_i)$$

And, we get the required refinement.

3. X has a basis of quasi-compact open sets follows from the above.

4. Let $Y \subseteq X$ be an irreducible closed subset. Then, $Y = \mathrm{Spec}(A/I)$. WLOG, we can assume X is irreducible. Next, observe that $\mathrm{Spec}(A) = \mathrm{Spec}(A_{\mathrm{red}}) = \mathrm{Spec}(A/\mathrm{Nil}(A))$. Since A is irreducible and reduced, we conclude that A is an integral domain. We are now done since 0 is a generic point in that case.

□

27. Lecture-2 (11th January, 2023): Zariski topology and affine schemes

27.1. Zariski topology contd..

Theorem 27.1.1 (Hochster)**.**
Every spectral space is homeomorphic to $\mathrm{Spec}(A)$ for some commutative ring A.

Notation: Ring be the category of commutative rings, **Top** be the category of topological spaces.

Theorem 27.1.2.
There is a contravariant functor

$$sp : \textbf{Ring} \to \textbf{Top}$$
$$\mathrm{Spec}(B) \mapsto \mathrm{Spec}(A)$$

Proof. Consider $f : A \to B$. This induces a map

$$f_{\#} : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

such that $f_{\#}(\mathfrak{p}) = f^{-1}(\mathfrak{p})$.
Well-defined: Suppose $xy \in f^{-1}(\mathfrak{p}) \Rightarrow f(xy) = f(x)f(y) \in \mathfrak{p} \Rightarrow$ either x or y lies in $f^{-1}(\mathfrak{p})$ which completes our check.
We claim that $f_{\#}$ is continuous. This can be seen as follows:
Take a basic open set $D(a), a \in A$. Enough to show for these sets since $D(a)$ forms a basis for the topology on $\mathrm{Spec}(A)$. Now,

$$\mathfrak{p} \in f_{\#}^{-1}(D(a)) \Leftrightarrow f_{\#}(\mathfrak{p}) \in D(a) \Leftrightarrow a \notin f^{-1}(\mathfrak{p})$$

But this means

$$a \notin f^{-1}(\mathfrak{p}) \Leftrightarrow f(a) \notin \mathfrak{p} \Leftrightarrow \mathfrak{p} \in D(f(a))$$

□

27.2. Affine schemes

Definition 27.2.1.
$\mathrm{Spec}(A)$ will be called an affine "scheme" (we will see this properly later on).

Definition 27.2.2.
Let $X = \mathrm{Spec}(A), Y = \mathrm{Spec}(B)$. Let $f : Y \to X$ be a continuous map. We call such a map f regular (holomorphic) if there is a ring homomorphism $g : A \to B$ such that $f = g_{\#}$

Example 27.2.3.
Take $\mathrm{Spec}(\mathbb{Z})$ and consider the constant map. This cannot be regular because any ring homomorphism must take 1 to 1 and as a consequence fixes every element.

Proposition 27.2.4.
If $X = \mathrm{Spec}(A)$. A regular function on X is a regular map from X to $\mathrm{Spec}(\mathbb{Z}[t])$.

Proof. □

Remark 27.2.5.
On an affine scheme, the set of all regular maps is the ring A itself since, the map $\mathbb{Z}[t] \to A$ is determined by where t is sent to.

Lemma 27.2.6.
Every affine scheme has a closed point.

Proof. Every commutative ring has a maximal ideal. □

Definition 27.2.7.
Open in affine is called quasi-affine.

Example 27.2.8.
Take A a local integral domain with $\mathfrak{m}$ the maximal ideal. Suppose that all prime ideals of A are of the form

$$\langle 0 \rangle \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \{\mathfrak{m}\}$$

Consider $X = \mathrm{Spec}(A) \backslash \mathfrak{m}$. X is open in affine scheme but has no closed point.

An example of such a ring is

$$\Gamma = \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \cdots$$

Give an ordering: $\sum a_i x_i \geq 0$ if the first nonzero term is > 0 or all $a_i = 0$
Γ is a totally ordered abelian group and hence there exists a valuation ring A with value group Γ and the prime ideals of Γ are in $1-1$ correspondence with prime ideals of A.

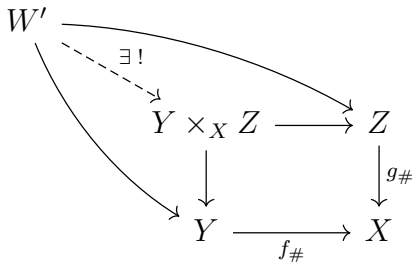
Exercise 27.2.9. *Let $A = k[X_1, X_2, \ldots], B = A_{\mathfrak{m}}, X = \mathrm{Spec}(B)\backslash\mathfrak{m}, \mathfrak{m} = \langle X_1, X_2, \ldots, \rangle$. Claim is that X has no closed point.*

27.2.1. Fiber products of affine schemes

Suppose A is a commutative ring, B, C are A-algebras. Let $X = \mathrm{Spec}(A), Y = \mathrm{Spec}(B), Z = \mathrm{Spec}(C)$. Next, suppose we have

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \\ C & & \end{array}$$

Universal property of fiber products:



Definition 27.2.10.
If a W exists such that the universal property is satisfied, then W is called the fiber product of Y, Z over X and we write $W = Y \times_X Z$

Theorem 27.2.11.
Aff$_{\mathbb{Z}}$ = category of affine schemes admits fiber products.

Proof. Consider the following data:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \\ C & & \end{array}$$

Let $D = B \otimes_A C$. We have the natural maps $f_1 : B \to B \otimes_A C$ sending $b \mapsto b \otimes 1$ and $f_2 : C \to B \otimes_A C$ sending $c \mapsto 1 \otimes c$. Both are ring homomorphisms and fit into the

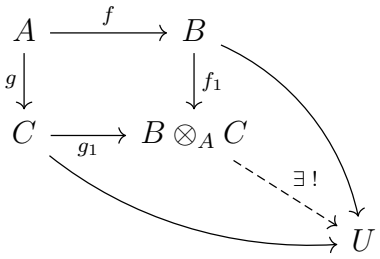
following diagram due to the nature of tensor product

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f_1} \\ C & \xrightarrow[g_1]{} & B \otimes_A C \end{array}$$

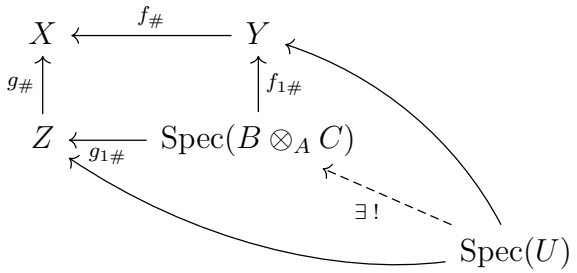
Now, let $W = \mathrm{Spec}(B \otimes_A C)$ and we claim that this satisfies the universal property of fibre product. Apply $\mathrm{Spec}(-)$ functor to the diagram to get

$$\begin{array}{ccc} A & \xleftarrow{f_\#} & B \\ {\scriptstyle g_\#}\uparrow & & \uparrow{\scriptstyle f_{1\#}} \\ C & \xleftarrow[g_{1\#}]{} & \mathrm{Spec}(B \otimes_A C) \end{array}$$

From the universal property of tensor product we have the following diagram



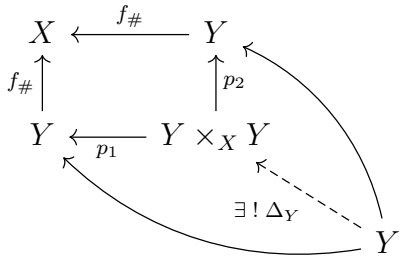
Again, apply the $\mathrm{Spec}(-)$ functor.



This completes the proof. □

28. Lecture-3 (16th January, 2023): Category theory brushup

Suppose we have a ring homomorphism $f : A \to B$ and $X = \mathrm{Spec}(A), Y = \mathrm{Spec}(B)$. This induces a map $f_\# : Y \to X$. From, the previous discussion, there is a fiber product $Y \times_X Y$ such that the following diagram makes sense



Here, $p_1 \circ \Delta_Y = p_2 \circ \Delta_Y = \mathrm{id}$ where

$$\Delta_Y : Y \to Y \times_X Y$$

is called the relative diagonal of Y/X.

Definition 28.0.1.
Say X_1, X_2 are affine schemes. $X_1 \to X_2$ is a closed immersion iff $A_1 \to A_2$ is a surjective. Here, $\mathrm{Spec}(A_i) = X_i, i = 1, 2$.

Lemma 28.0.2.
Δ_Y is a closed immersion.

Proof. $B \otimes_B B \to B$ is a surjection. □

Example 28.0.3.
Take $A = \mathbb{Z}, B = \mathbb{Z}[t]/\langle t^n \rangle$ for some $n \geq 2$. There is a canonical inclusion $f : A \to B$. This induces a map $Y = \mathrm{Spec}(B) \to X = \mathrm{Spec}(A)$ which is an identity map in terms of sets. Thus, it is a closed inclusion but not a closed immersion.

Remark 28.0.4.
We know that diagonal is closed iff the space is Hausdorff. This seems to contradict our assumptions! But we are fine because this claim is true only when the topology

is the product topology. Here, the topology we have is not the product topology.

Definition 28.0.5.
A regular map $f : X \to Y$ is called separated morphism if the relative diagonal of Y over X is closed in $Y \times_X Y$.

Lemma 28.0.6.
Let $X = \mathrm{Spec}(A)$. Suppose U_1, U_2 are two open affine subsets of X. Then, $U_1 \cap U_2$ is also affine.

Proof. We have two natural injections

$$U_1 \overset{j_1}{\hookrightarrow} X, U_2 \overset{j_2}{\hookrightarrow} X$$

then we naturally have the following

$$U_1 \times_Z U_2 \xrightarrow{j_1 \times j_2} X \times_Z X$$

where $Z = \mathrm{Spec}(\mathbb{Z})$ (if it is blank, just assume Z by default).
From previous discussion we get

$$\begin{array}{ccc} U_1 \times_Z U_2 & \xrightarrow{j_1 \times j_2} & X \times_Z X \\ & & \uparrow{\scriptstyle \Delta_X} \\ & & X \end{array}$$

Since each term is affine, we can take the fiber product of $U_1 \times_Z U_2$ and X. Say the fiber product is W.

$$\begin{array}{ccccccc} & & U_2 & & X & & \\ & & \uparrow{\scriptstyle q_1} & & \uparrow{\scriptstyle p_1} & & \\ U_1 & \xleftarrow{q_2} & U_1 \times_Z U_2 & \xrightarrow{j_1 \times j_2} & X \times_Z X & \xrightarrow[p_2]{} & X \\ & & \uparrow{\scriptstyle \Delta'} & \square & \uparrow{\scriptstyle \Delta_X} & & \\ & & W & \xrightarrow[j]{} & X & & \end{array}$$

Then, we claim that

Claim: $W = U_1 \cap U_2$

Proof. Suppose $x \in W$, then $\square$

It now remains to show that W is affine but it is clear from the definition of fiber products.

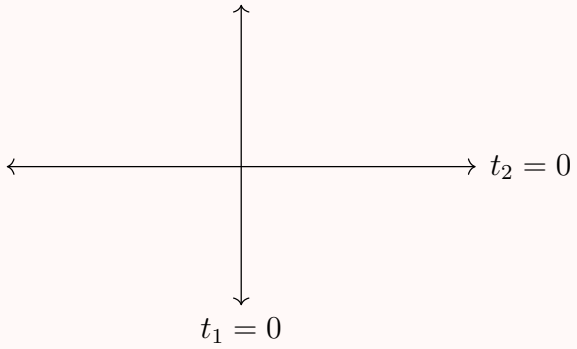
□

Remark 28.0.7.
If Δ_X is a closed immersion then so is Δ'. That is, closed immersions are preserved under fiber products. Follows from right exactness of tensor product.

Now, that we have discussed intersection, we naturally ask : What happens to $U_1 \cup U_2$. Is it still affine ?

The answer turns out to be NO. To see this,

Example 28.0.8 (NON-example)**.**
Consider k be an algebraically closed field. $A = k[t_1, t_2]$ and $X = \mathrm{Spec}(A)$. Let $U_i = \{x \mid t_i(x) \neq 0\} = X \backslash \mathcal{V}(t_i)$. Clearly, U_i is open and affine ($= \mathrm{Spec}(A_{t_i})$). But $U_1 \cup U_2$ is not affine.



U_1 is complement of the horizontal axis and U_2 of the vertical axis. But $U_1 \cup U_2$ is the complement of origin. The question is asking if the complement of origin is affine or not. A highly NON-TRIVIAL question to answer.

Exercise 28.0.9 (not trivial but do think about it)**.** *Suppose $X = \mathrm{Spec}(A)$ and $U \hookrightarrow X$ is affine open. Does this imply $U = \mathrm{Spec}(S^{-1}A)$ for some multiplicatively closed set $S \subseteq A$?*

Definition 28.0.10.
Suppose $S = \mathrm{Spec}(A)$ and $x \in X$. Let $K(A) = S^{-1}(A)$ where S is the set of all nonzero divisors in A. Here, we have $A \hookrightarrow S^{-1}(A) =$ the ring of all meromorphic functions on X. Then,

$$\mathcal{O}_{X,x} = \{f \in K(A) \mid f \text{ is regular in a nbd of } x\}$$

is called the germ of regular function.

Lemma 28.0.11.

$$\mathcal{O}_{X,x} = A_{\mathfrak{p}}$$

where $\mathfrak{p} = x$.

Proof. Suppose f is regular in a nbd of $\mathfrak{p}$ iff there exists $b \notin \mathfrak{p}$ such that $f \notin \mathcal{V}(b)$. But this means $f \notin A_b$ which in turn implies $f \in \bigcup_{b \notin \mathfrak{p}} A_b = A_{\mathfrak{p}}$. □

Definition 28.0.12.
The germs of analytic functions at x is the completion of $\mathcal{O}_{X,x}$, denoted by $\mathcal{O}^{\wedge}_{X,x}$ with respect to its maximal ideal.

Remark 28.0.13.
We have the natural map $\mathcal{O}_{X,x} \to \mathcal{O}^{\wedge}_{X,x}$ but if $\mathcal{O}_{X,x}$ is Noetherian then this map is also injective.

28.1. Categories and functors

A category $\mathcal{C}$ consists of a collection $\mathrm{ob}(\mathcal{C})$ and for all $X, Y \in \mathrm{ob}(\mathcal{C})$, there is a set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ and a map

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

satisfying

1. $\forall\ X \in \mathrm{ob}(\mathcal{C})\ \exists\ 1_X \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ such that $f \circ 1_X = 1_X \circ f = f$
2. $f \circ (g \circ h) = (f \circ g) \circ h$

A functor (contravariant) $\mathcal{F} : \mathcal{C}_1 \to \mathcal{C}_2$ is a function $\mathcal{F} : \mathrm{ob}(\mathcal{C}_1) \to \mathrm{ob}(\mathcal{C}_2)$ and a map of sets $\mathcal{F} : \mathrm{Hom}_{\mathcal{C}_1}(X, Y) \to \mathrm{Hom}_{\mathcal{C}_2}(\mathcal{F}(X), \mathcal{F}(Y))$ such that

1. $f(1_X) = 1_{\mathcal{F}(X)}$
2. $\mathcal{F}(f \circ g) = \mathcal{F}(f) \circ \mathcal{F}(g)$

To each category $\mathcal{C}$, we associate a category $\mathcal{C}^{\mathrm{op}}$ such that

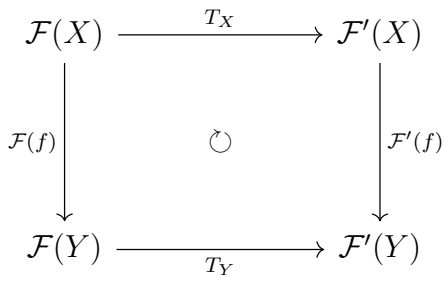
$$\mathrm{ob}(\mathcal{C}) = \mathrm{ob}(\mathcal{C}^{\mathrm{op}})$$

and

$$\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$$

Suppose $\mathcal{F}, \mathcal{F}' : \mathcal{C} \to \mathcal{C}'$ be two functors. Then, a natural transformation is $T : \mathcal{F} \to \mathcal{F}'$ consisting of the following data:

1. $\forall\ X \in \mathcal{C}, \exists\ T_X : \mathcal{F}(X) \to \mathcal{F}'(X)$,i.e., $T_X \in \mathrm{Hom}_{\mathcal{C}'}(\mathcal{F}(X), \mathcal{F}'(X))$ such that for all $f : X \to Y$, the diagram commutes



Given, $\mathcal{C}, \mathcal{C}'$ then $F(\mathcal{C}, \mathcal{C}') =$ all functors from $\mathcal{C}$ to $\mathcal{C}'$ is a category and $\mathrm{Hom}_{F(\mathcal{C},\mathcal{C}')}(F_1, F_2) =$ all natural transformations from F_1 to F_2

29. Lecture-4 (20th January, 2023): Category theory

29.1. Category theory contd..

29.1.1. Equivalence of categories

Two categories $\mathcal{C}, \mathcal{C}'$ are equivalent if there exists functors

$$\mathcal{F} : \mathcal{C} \to \mathcal{C}' \text{ and } \mathcal{G} : \mathcal{C}' \to \mathcal{C}$$

and natural transformations

$$T : \mathrm{id}_{\mathcal{C}} \to \mathcal{G} \circ \mathcal{F} \text{ and } T' : \mathrm{id}_{\mathcal{C}'} \to \mathcal{F} \circ \mathcal{G}$$

which are isomorphisms.

Example 29.1.1.
1. The category of categories with all morphisms being identity is equivalent to the category of sets.
2. The category
3. Consider the category of A-modules and let $B = M_n(A)$. We claim that $\mathbf{Mod}_{\mathrm{A}}$ and $\mathbf{Mod}_{\mathrm{B}}$ are equivalent. This is also known as Morita equivalence.

29.1.2. Products and Co-products

In partially ordered sets, neither product nor co-product might exist.

29.2. Pre-sheaves and Yoneda lemma

Suppose $\mathcal{C}$ is a category. Then a presheaf on $\mathcal{C}$ is a contravariant functor

$$\mathcal{F} : \mathcal{C} \to \mathbf{Sets}(\text{ or } \mathbf{Ab})$$

The category of presheaves on $\mathcal{C}$ is denoted by $\mathbf{Presh}(\mathcal{C})$

Suppose $X \in \mathrm{ob}(\mathcal{C})$. Then we can construct $h_X \in \mathbf{Presh}(\mathcal{C})$ such that $h_X(Y) =$

$\mathrm{Hom}_{\mathcal{C}}(Y, X)$. Hence, we have a functor

$$h : \mathcal{C} \to \mathbf{Presh}(\mathcal{C})$$

that sends $X \mapsto h_X$. This h is called the Yoneda functor.

Lemma 29.2.1 (Yoneda Lemma)**.**
For every pre-sheaf F on $\mathcal{C}$ and for all $X \in \mathrm{ob}(\mathcal{C})$, there exists a natural bijection

$$\theta_X : \mathrm{Hom}_{\mathbf{Presh}(\mathcal{C})}(h_X, F) \to F(X)$$

Proof. Suppose we are given $f : h_X \to F$. This is a natural transformation and thus we obtain

$$f(X) : h_X(X) \to F(X)$$

but $h_X(X) = \mathrm{Hom}_{\mathcal{C}}(X, X)$ and $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$. This implies $f(X)(\mathrm{id}_X) \in F(X)$ and therefore $\theta_X(f) = f(X)(\mathrm{id}_X) \in F(X)$.
Now, let us construct the inverse. Construct

$$\psi_X : F(X) \to \mathrm{Hom}_{\mathbf{Presh}(\mathcal{C})}(h_X, F)$$

Let $\alpha \in F(X)$, we want to define

$$h_X(Y) \to F(Y) \; \forall \; Y \in \mathcal{C}$$

But then $f \in h_X(Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$ implies $F(X) \xrightarrow{F(f)} F(Y) \Rightarrow F(f)(\alpha) \in F(Y)$.
We can easily check that these two maps are inverses which completes the proof. □

Suppose $\mathcal{F} : \mathcal{C} \to \mathcal{C}'$ is a functor. Then, $\mathcal{F}$ is called faithful if

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \hookrightarrow \mathrm{Hom}_{\mathcal{C}'}(\mathcal{F}(X), \mathcal{F}(Y)) \; \forall \; X, Y \in \mathrm{ob}(\mathcal{C})$$

We say that $\mathcal{F}$ is full if this map is an epimorphism and $\mathcal{F}$ is an embedding if $\mathcal{F}$ is fully faithful.

Lemma 29.2.2.
Yoneda functor is an embedding.

Proof. By Yoneda lemma we have

$$\mathrm{Hom}_{\mathbf{Presh}(\mathcal{C})}(h_X, h_Y) = h_Y(X)$$

But since $h_Y(X) = \mathrm{Hom}_{\mathcal{C}}(X, Y)$, the proof is complete. □

29.2.1. Adjoint functors

Suppose we have two functors

$$\mathcal{F} : \mathcal{C} \to \mathcal{C}' \text{ and } \mathcal{G} : \mathcal{C}' \to \mathcal{C}$$

The pair $(\mathcal{F}, \mathcal{G})$ is an adjoint pair if for all $X \in \mathrm{ob}(\mathcal{C})$ and $Y \in \mathrm{ob}(\mathcal{C}')$, there exists a natural transformation

$$\mathrm{Hom}_{\mathcal{C}}(X, \mathcal{G}(Y)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}'}(\mathcal{F}(X), Y)$$

Example 29.2.3. 1.

2.

Proposition 29.2.4.
Left adjoint and right adjoint have to be unique (if they exist).

Suppose we have an adjoint pair $(\mathcal{F}, \mathcal{G})$. Then, for every $X \in \mathrm{ob}(\mathcal{C})$ we have (follows from adjoint-ness)

$$\mathrm{Hom}_{\mathcal{C}}(X, \mathcal{G} \circ \mathcal{F}(Y)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}'}(\mathcal{F}(X), \mathcal{F}(Y))$$

This implies there is a canonical map

$$u_X : X \to \mathcal{G} \circ \mathcal{F}(X)$$

and this in turn implies the existence of a natural transformation

$$u : \mathrm{id}_{\mathcal{C}} \to \mathcal{G} \circ \mathcal{F}$$

called the unit of adjunction.
Similarly, for all $Y \in \mathrm{ob}(\mathcal{C}')$ we have

$$\mathrm{Hom}_{\mathcal{C}}(\mathcal{F} \circ \mathcal{G}(X), Y) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}'}(\mathcal{G}(Y), \mathcal{G}(Y))$$

This implies the existence of a natural transformation

$$\epsilon : \mathrm{id}_{\mathcal{C}'} \to \mathcal{G} \circ \mathcal{F}$$

called the co-unit of adjunction.

Definition 29.2.5.
It is a category $\mathcal{C}$ such that

1. it admits finite coproduct.
2. it has a zero product (both final and initial object).
3. $\mathrm{Hom}_{\mathcal{C}}(X, Y) \in \mathbf{Ab}$ such that

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

is bilinear.

Definition 29.2.6.
It is an additive category such that every map $f : X \to Y$ has a kernel and a cokernel.

30. Lecture-5 (23rd January, 2023): Etale morphisms

Let A be a commutative ring and M be a A-module.

Definition 30.0.1.
M is flat if

$$N \hookrightarrow N' \Rightarrow N \times M \hookrightarrow N' \times M$$

Definition 30.0.2.
M is faithfully-flat if M is flat and

$$N = 0 \Leftrightarrow N \times_A M = 0$$

Definition 30.0.3.
M is projective if it is a direct summand of a free A-module. Or equivalently,

$$N \twoheadrightarrow N' \Rightarrow \mathrm{Hom}(M, N) \twoheadrightarrow \mathrm{Hom}(M, N')$$
$$\Leftrightarrow \mathrm{Ext}^i_A(M, N) = 0 \; \forall i > 0 \; \forall \; N$$

Lemma 30.0.4.
Suppose A is Noetherian and M is a finitely generated A-module. TFAE:

1. M is projective.
2. M is flat.
3. $M_{\mathfrak{m}}$ is flat for all maximal ideals $\mathfrak{m}$.
4. $M_{\mathfrak{m}}$ is free for all maximal ideals $\mathfrak{m}$.

Proof. □

Let k be a field and A a k-algebra.

Definition 30.0.5.
A is called separable over k if $A \otimes_k k'$ is reduced for all field extensions k'/k.

Lemma 30.0.6.
A is separable over k iff every finitely generated subalgebra is separable over k.

Proposition 30.0.7.
Assume that A is finite dimensional over k. TFAE:

1. A is separable over k.
2. $\overline{A} := A \otimes_k \overline{k} = \prod_{i=1}^{n} \bar{k}$.
3. $A = \prod_{i=1}^{n} k_i$ where k_i/k is a finite separable field extension.
4. The trace form $A \times A \to k((w, w') \mapsto \mathrm{Tr}_{A/k}(ww'))$ is non-degenerate.

Proof. □

30.1. Kahler Differentials

Let A be a commutative ring and M an A-module. A derivative $D : A \to M$ is an abelian group homomorphism such that

$$D(ab) = aD(b) + D(a)b$$

Let

$$\mathrm{Der}(A, M) = \text{ the set of derivations from } A \text{ to } M$$

If A is a k-algebra where k is a commutative ring, then we say that D is a k-derivation if $D(k) = 0$

More notation: Let $\mathrm{Der}_k(A, M)$ be the set of all k-derivations and $\mathrm{Der}_k(A) = \mathrm{Der}_k(A, A)$

We can make $\mathrm{Der}(A, M)$ is an A-module so that

$$(a \cdot D)(b) = aD(b)$$

Suppose

$$D : A \to M$$

then

$$D(\mathbb{Z}) = 0$$
$$\mathrm{Der}(A, M) = \mathrm{Der}_{\mathbb{Z}}(A, M)$$

Take $D, D' \in \mathrm{Der}_k(A)$, then we can define the bracket $[-,-]$ as

$$[D, D'] = DD' - D'D$$

This converts $\mathrm{Der}_k(A)$ into a Lie algebra

Remark 30.1.1.
1. $d(a^n) = na^{n-1}d(a)$
2. $d^n(ab) = \sum_{i=0}^{n} \binom{n}{i} d^i a d^{n-i} b$

In particular, if $\mathrm{char}(A) = p > 0$ then

1. $d^p(ab) = ad^p b + bd^p(a) \Rightarrow d^p$ is a k-derivation.
2. $d^p(a+b) = d^p a + d^p b$

Clearly, $\mathrm{Der}_k(A, -) : A - \mathrm{mod} \to A - \mathrm{mod}$ is a covariant functor.

Proposition 30.1.2.
$\mathrm{Der}_k(A, -)$ is a representable functor.

Proof. □

31. Lecture-6 (25th January, 2023):Kahler Differentials

31.1. Differentials and Derivations

Theorem 31.1.1.
There exists an unique A-module (upto isomorphism) $\Omega'_{A/k}$ with a k-derivation $d_{A/k} : A \to \Omega'_{A/k}$ such that for all A-modules M and a k-derivation $D : A \to M$, $\exists! A$-linear map $\varphi : \Omega'_{A/k} \to M$ such that $D = \varphi \circ d_{A/k}$

$$\mathrm{Der}_k(A, M) \xrightarrow{\sim} \mathrm{Hom}_A(\Omega'_{A/k}, M)$$

Proof. □

Definition 31.1.2.
A square zero extension of k-algebras is a surjection of k-algebras $g : B \twoheadrightarrow C$ such that $M^2 = 0$ where $M = \ker(g)$.
We can think of B as the manifold C plus some other tangent directions. B is some kind of thickening of C in the spec level.

Example 31.1.3.
Suppose $M \in \mathbf{Mod}_A$ and $B = A \oplus M$. Addition and multiplication are defined as follows:

$$(a, m) + (a', m') = (a + a', m + m')$$
$$(a, m) \cdot (a', m') = (aa', am' + a'm)$$

Here,

$$0 \longrightarrow M \longrightarrow B \xrightarrow{\varphi} A \longrightarrow 0$$

$$(a, m) \longmapsto a$$

is a square zero extension. We wish to ask when does the following lift exist.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & B & \xrightarrow{\varphi} & C & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle ?} & \nearrow_{g} & & & \\ & & & & A & & & & \end{array}$$

Suppose we are given a lift $h : A \to B$ of g and h' is another lift of g. Then,

$$\begin{array}{ccc} D := h - h' : A & \longrightarrow & B \\ & \searrow & \uparrow \\ & & M \end{array}$$

M is a C-module ($M = M/M^2 = M \otimes B/M = C$ is a C-module). So, M is also an A-module via the map g.

Claim: $D \in \mathrm{Der}_k(A, M)$

Proof. □

Conversely, if $D \in \mathrm{Der}_k(A, M)$, then $h' = h + D$ is also a lift.

Proof of main theorem. 1. Consider the map $A \otimes_k A \xrightarrow{\mu} A$ such that $a \otimes b \mapsto ab$. μ is a surjective k-algebra homomorphism. Let $I = \ker(\mu)$ and $B = A \otimes_k A/I^2$. We obtain the following square zero extension

$$0 \longrightarrow I/I^2 \longrightarrow B \xrightarrow{\varphi} A \longrightarrow 0$$

Let $\Omega'_{A/k} := I/I^2$ is the module of Kahler differentials.
$\Omega_{A/k}$ the canonical sheaf of diagonal embedding of $X \hookrightarrow X \times X$
Define

$$\begin{aligned} \alpha_1 : A \to B \alpha_1(a) &= a \otimes 1 \pmod{I^2} \\ \alpha_2 : A \to B \alpha_2(a) &= 1 \otimes a \pmod{I^2} \end{aligned}$$

We obtain the following diagram that commutes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Omega'_{A/k} & \longrightarrow & B & \xrightarrow{\varphi} & A & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle \alpha_i} & \nearrow{\scriptstyle \mathrm{id}} & & & \\ & & & & A & & & & \end{array}$$

Next, define $d_{A/k} = \alpha_1 - \alpha_2$.
Let $M \in \mathbf{Mod}_A$ and $D : A \to M$ a k-derivation.
Now, define

$$\begin{aligned} \theta : A \otimes_k A \to A * M (= A \oplus M) \text{ a square zero extension} \\ a \otimes b \mapsto (ab, aDb) \end{aligned}$$

Claim: $\theta(I) \hookrightarrow M$

Proof. Suppose $\sum x_i \otimes y_i \in I \Rightarrow \sum x_i y_i = 0 \in A$. This implies $\theta(\sum x_i \otimes y_i) =$

$(\sum x_i y_i = 0, \sum x_i D y_i) \in M$. Therefore,

$$\theta(I/I^2) \hookrightarrow M/M^2 = M$$

Thus θ descends to a map

$$\tilde{\theta} : I/I^2 \to M$$

or $\tilde{\theta} : \Omega'_{A/k} \to M$ □

Claim: $\tilde{\theta}$ is unique such that $\tilde{\theta} \circ d_{A/k} = D : A \to M$

Proof. Suffices to show that $\Omega'_{A/k}$ is generated by $\langle da : a \in A \rangle$ as an A-module.

$$\begin{aligned} a \otimes a' &= (a \otimes 1)(-a' \otimes 1 + 1 \otimes a') + aa' \otimes 1 \\ \alpha \in \Omega'_{A/k} &\Rightarrow \alpha = \sum x_i \otimes y_i \qquad \text{such that } \sum x_i y_i = 0 \\ &\Rightarrow \alpha = \sum x_i dy_i \end{aligned}$$

□

□

Corollary 31.1.4.

$$\Omega'_{A/k} = \frac{\text{free module on } da}{\text{additivity + Leibnitz rule}}$$

In particular, $\mathrm{Der}_k(A) = \Omega'^{*}_{A/k} = \mathrm{Hom}(\Omega'_{A/k}, A) = T_{A/k}$ (tangent space)

Definition 31.1.5.
We say that A is formally smooth over k if given any square zero extension

$$0 \longrightarrow M \longrightarrow B \xrightarrow{\varphi} A \longrightarrow 0$$

and a diagram of k-algebras, there exists a lifting $\tilde{g}$ of g

$$\begin{array}{ccc} k & \xrightarrow{f} & C \\ \downarrow & \overset{\tilde{g}}{\swarrow} & \downarrow g \\ B & \xrightarrow[\varphi]{} & A \end{array}$$

Definition 31.1.6.
We say that A is formally unramified over k if g has atmost one lift.
We say that A is formally étale over k if A is formally smooth and formally unramified.

Definition 31.1.7.
We say that A is smooth (resp. unramified, étale) if it is formally smooth (unramified, étale) and finite type over k.

Exercise 31.1.8. $A = k[X_1, \ldots, X_n], \Omega'_{A/k} = ?$
***Claim**: There is a canonical isomorphism of A-modules*

$$\theta : \underbrace{AdX_1 \oplus \cdots \oplus AdX_n}_{F} \xrightarrow{\sim} \Omega'_{A/k}$$

Lemma 31.1.9.
Suppose $U \subseteq A$ is any set that generates A as k-algebra. Then, $\Omega'_{A/k}$ is generated by $\{da : a \in A\}$ as A-module.

Proof. □

This lemma implies the map is surjective.
Next, define $D_i : A \to A$ such that $f \mapsto \dfrac{\partial d}{\partial x_i}(f)$.
This gives an unique A-linear map $\psi_i : \Omega'_{A/k} \to A$. Define $\psi : \Omega'_{A/k} \to F$ such that $\psi = \sum_{i=1}^{n} \psi_i$. This implies $\psi \circ \theta = \mathrm{id}_F$. Hence, ψ is injective.

32. Lecture-7 (30th January, 2023): Module of differentials

Lemma 32.0.1.
A is formally unramified iff $\Omega^1_{A/k} = 0$.

Proof. Suppose that $\Omega^1_{A/k} = 0$. Let

$$0 \longrightarrow M \longrightarrow B \xrightarrow{\varphi} C \longrightarrow 0$$

be a square zero extension. We had seen that all liftings of $f : A \to C$ differ by $\mathrm{Der}_k(A, M) = \mathrm{Hom}_A(\Omega^1_{A/k}, M)$. This implies there is atmost one lifting of f and this concludes what we want.

For the other direction, suppose A is formally unramified over k. Recall

$$\mu : A \otimes_k A \to A$$

$$I = \ker(\mu)$$

and

$$0 \longrightarrow I/I^2 = \Omega^1_{A/k} \longrightarrow B = (A \otimes_k A)/I^2 \xrightarrow{\varphi} C \longrightarrow 0$$

We had two liftings from A to B, α_1, α_2 namely $\alpha_1(a) = a \otimes 1, \alpha_2(a) = 1 \otimes a$ and $d_{A/k} = \alpha_1 - \alpha_2$. Since A is formally unramified, $d_{A/k} = 0$ which implies $\Omega^1_{A/k} = 0$. □

Exercise 32.0.2. *Suppose K/k be a finite separable extension. We claim that this extension is formally unramified.*

Lemma 32.0.3.
If $k \xrightarrow{f} A$ is of finite type (k is a ring), then $\Omega^1_{A/k}$ is a finitely generated A-module.

Proof. □

Example 32.0.4.
If A is a commutative ring, S a multiplicatively closed subset of A, $B = S^{-1}A$. Then, $A \to B$ is formally etale.

Formally unramified: Enough to show that

$$d_{A/k}(fg^{-1}) = 0 \; \forall \; f \in A, g \in S$$

But this means

$$\begin{aligned} d_{B/A}(fg^{-1}) &= fd_{A/B}(g^{-1}) + g^{-1}d_{B/A}(f) \\ &= fd_{A/B}(g^{-1}) \\ gd_{A/B}(g^{-1}) + g^{-1}d_{A/B}(g) &= 0 \\ \Rightarrow gd_{A/B}(g^{-1}) &= 0 \\ \Rightarrow d_{B/A}(g^{-1}) &= 0 \end{aligned}$$

Next,
Formally unramified:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & C & \xrightarrow{\varphi} & C' & \longrightarrow & 0 \\ & & & \nearrow^{g} & \uparrow{\scriptstyle \tilde{f}} & \nearrow_{f} & & & \\ & & A & \xrightarrow[\theta]{} & B & & & & \end{array}$$

$$\begin{aligned} \tilde{f} \text{ exists } &\Leftrightarrow g(s) \in C^{\times} \; \forall \; g \in S \\ &\Leftrightarrow \varphi g(s) = f\theta(s) \in C'^{\times} \end{aligned}$$

Then use the lemma stated after this example.

Lemma 32.0.5.
If

$$0 \longrightarrow I \longrightarrow C \xrightarrow{\varphi} C' \longrightarrow 0$$

is an extension of rings such that I is nilpotent. Then $a \in C^{\times} \Leftrightarrow \varphi(a) \in C'^{\times}$.

Proof. □

Theorem 32.0.6 (First fundamental theorem for module of differentials)**.**
Let

$$k \xrightarrow[f]{} A \xrightarrow[g]{} B$$

be ring homomorphisms. Then,

$$\Omega^1_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega^1_{B/k} \xrightarrow{\beta} \Omega^1_{B/A} \longrightarrow 0$$

is exact. Moreover, it is split exact if B is formally smooth over A. Here, $\alpha(ad_{A/k}a' \otimes b') = bad_{B/k}(a'), \beta(ad_{B/k}b) = ad_{B/A}(b)$.

Proof. We know that a sequence of B-modules

$$N' \longrightarrow N \longrightarrow N''$$

is exact iff

$$\mathrm{Hom}_B(N'', M) \longrightarrow \mathrm{Hom}_B(N, M) \longrightarrow \mathrm{Hom}_B(N', M)$$

is exact for all B-module M.

Thus, we just need to check that

$$\mathrm{Hom}_B(\Omega^1_{B/A}, M) \longrightarrow \mathrm{Hom}_B(\Omega^1_{B/k}, M) \longrightarrow \mathrm{Hom}_B(\Omega^1_{A/k} \otimes_A B, M) = \mathrm{Hom}_A(\Omega^1_{A/k}, M)$$

is exact. But this is equivalent to checking

$$\mathrm{Der}_A(B, M) \xrightarrow{\beta^*} \mathrm{Der}_k(B, M) \xrightarrow{\alpha^*} \mathrm{Der}_k(A, M)$$

is exact.

Next, assume that B is formally smooth over A. We need to show that α^* is surjective. Let $D \in \mathrm{Der}_k(A, M)$. We know that the diagram

$$\begin{array}{ccc} B & \xrightarrow{\mathrm{id}} & B \\ {\scriptstyle g}\uparrow & & \uparrow{\scriptstyle p_1} \\ A & \xrightarrow[\varphi]{} & B * M = B \oplus M \end{array}$$

commutes. But $B * M$ is a square zero extension. Thus, we get a map $B \to B * M$ such that diagram

$$\begin{array}{ccc} B & \xrightarrow{\mathrm{id}} & B \\ {\scriptstyle g}\uparrow & \overset{\theta}{\searrow} & \uparrow{\scriptstyle p_1} \\ A & \xrightarrow[\varphi]{} & B * M = B \oplus M \end{array}$$

commutes. Here, $\varphi(a) = (ga, Da)$. We write $\theta(b) = (b, D'b)$.

Claim: D' is a k-derivation from B to M.

It is clear that $D' \circ g = D$. This is equivalent to a B-linear map $\alpha' : \Omega^1_{B/k} \to M$. Define

$$D : A \to \Omega^1_{A/k} \otimes_A B$$
$$D(a) = d_{A/k}(a) \otimes 1$$

Check that $D \in \mathrm{Der}_k(A, \Omega^1_{A/k} \otimes_A B)$. This implies the existence of an extension $D' : B \to \Omega^1_{A/k} \otimes_A B$ such that $D' \circ g = D$ iff a B-linear map $\alpha' : \Omega^1_{B/k} \to \Omega^1_{A/k} \otimes_A B$ such that $\alpha' \circ g = \alpha$.

Claim: $\alpha' \circ \alpha = \mathrm{id}$

This concludes the proof. □

Suppose

$$k \xrightarrow{f} A \xrightarrow{g} B$$

From the previous theorem, we get

$$\Omega^1_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega^1_{B/k} \xrightarrow{\beta} \Omega^1_{B/A} = 0 \longrightarrow 0$$

is exact. Or rather

$$\Omega^1_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega^1_{B/k} \longrightarrow 0$$

is exact. What is the kernel of this map?

Theorem 32.0.7 (Second fundamental theorem of module of differentials)**.** Let $I = \ker(A \twoheadrightarrow B)$. Then, there exists an exact sequence

$$I/I^2 \xrightarrow{\delta} \Omega^1_{A/k} \otimes_A B \longrightarrow \Omega^1_{B/k} \longrightarrow 0$$

where $\delta(a) = d_{A/k}(a) \otimes 1$. Moreover, this sequence is split exact if B is formally smooth over k.

Example 32.0.8.
Let $B = k[X_1, X_2, \ldots, X_n]/\langle f_1, \ldots, f_n \rangle$. Then, what is $\Omega^1_{B/k}$.

If $A = k[X_1, X_2, \ldots, X_n]$. Then,

$$\Omega^1_{A/k} = A dx_1 \oplus \cdots \oplus A dx_n$$

$X = \mathrm{Spec}(A), Y = \mathrm{Spec}(B = A/I)$

33. Lecture-8 (1st February, 2023):

Part V.

Topics in Analytic Number Theory

34. Lecture-l: Hardy-Littlewood proof of infinitely many zeros on the line $\mathfrak{R}(s) = 1/2$

35. Lecture-2:

36. Lecture-3 (10th January, 2023): Siegel's theorem

Theorem 36.0.1 (Siegel)**.**
Let $\chi(q)$ be a real Dirichlet character modulo $q \geq 3$. Given any $\epsilon > 0$, we have

$$L(1,\chi) \geq \frac{C_\epsilon}{q^\epsilon}$$

A trivial lower bound: $L(1,\chi) \gg q^{-1/2}$

Goldfeld's proof. Consider

$$f(s) = \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2)$$

with $\chi_i, i = 1,2$ primitive quadratic characters. Notice that $f(s) = \sum_n b_n n^{-s}$ with $b_1 = 1, b_n \geq 0$. Let $\lambda = \text{Res}_{s=1} f(s) = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2)$

Lemma 36.0.2.
Given any $\epsilon > 0$, one can find $\chi_1(q_1)$ and β with $1-\epsilon < \beta < 1$ such that $f(\beta) \leq 0$, independent of what $\chi_2(q_2)$ is.

Proof. **Case-1:** If there are no real zeros of $L(s,\psi)$ for any primitive quadratic character in $(1-\epsilon, 1)$, then $f(\beta) < 0$ for any $\beta \in (1-\epsilon, 1)$. This is because

$$f(\beta) = \underbrace{\zeta(\beta)}_{<0}\underbrace{L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2)}_{>0}$$

as $L(1,\chi) > 0$ and L is continuous so any change of sign will lead to a zero which is a contradiction.
Case-2: If we cannot find such a ψ, then just set $\chi_1 = \chi$ and let β be the real zero. Then, $f(\beta) = 0$. We are done. □

Next, consider the integral

□

Corollary 36.0.3.

$$\begin{aligned} h(-d) &= \frac{L(1,\chi_d)\sqrt{|d|}\,\omega}{2\pi} \\ &= \frac{L(1,\chi_d)}{\log \epsilon_d} \end{aligned}$$

Theorem 36.0.4 (Y. Zhang)**.**

$$L(1,\chi) \geq \frac{c}{(\log q)^{2022}}$$

Theorem 36.0.5.
If $\chi(q)$ does not have a Siegel zero, then $L(1,\chi) \gg \frac{1}{\log q}$

37. Lecture-4 (12th January, 2023): PNT for Dirichlet characters and APs

Lemma 37.0.1.
If $\rho = \beta + i\gamma$ runs through nontrivial zeros of $L(s, \chi)$, then

$$\sum_{\rho} \frac{1}{1 + (T - \gamma)^2} = \mathcal{O}(\log q(|T| + 2)) \forall T \in \mathbb{R}$$

Lemma 37.0.2.

$$N(T + 1, \chi) - N(T, \chi) = \mathcal{O}(\log q(|T| + 2))$$

Lemma 37.0.3.

$$\sum_{\rho : |\gamma - t| \leq 1} \frac{1}{s - \rho} + \mathcal{O}(\log qt) = \frac{L'}{L}(s, \chi)$$

for $-1 \leq \sigma \leq 2, |t| \geq 2, L(s, \chi) \neq 0$

Lemma 37.0.4.
Let $\chi(q)$ be primitive, $q \geq 3, T \geq 2$. Then, there exists $T_1 \in [T, T + 1]$ such that $\frac{L'}{L}(\sigma \pm iT_1, \chi) \ll (\log qT)^2, -1 \leq \sigma \leq 2$.

Lemma 37.0.5.
Put $a = 1$ if χ is even and 0 otherwise.

$$\mathcal{A}(a) := \{s \in \mathbb{C} \mid \sigma \leq -1, |s + 2n - a| \geq \frac{1}{4} \forall\, n \geq 1\}$$

Then,

$$\frac{L'}{L}(s, \chi) \ll \log(q(|s| + 1))$$

on $\mathcal{A}(a)$

These are all the ingredients needed to prove the the explicit formula for $\psi_0(x, \chi)$.

Theorem 37.0.6.

$$\psi(s,\chi) = \sum_{n\leq x} \Lambda(n)\chi(n)$$

$$\psi_0(x,\chi) = \frac{1}{2}(\psi(x^+,\chi)+\psi(x^-,\chi)) = -\sum_{\rho:|\gamma|\leq t} \frac{x^\rho}{\rho} - \frac{1}{2}\log(x-1) - \frac{\chi(-1)}{2}\log(x+1) + C_\chi + R_\chi(T)$$

where $C_\chi = \frac{L'}{L}(1,\overline{\chi}) + \log\frac{q}{2\pi} - \gamma$ and $R_\chi(T) \ll (\log x)\min(1, x/T < x >) + \frac{x}{T}(\log(qxT))^2$. Letting $T \to \infty$ we see that $R_\chi(T) \to 0$.

Theorem 37.0.7 (Brun-Titsmarsh inequality)**.**
Let $x \geq 0, y \geq 2q$. Then,

$$\pi(x+y;q,a) - \pi(x;q,a) \leq \frac{2y}{\phi(q)\log(\frac{y}{q})}\left(1 + \mathcal{O}(\frac{1}{\log(\frac{y}{q})})\right)$$

Remind him to prove this later; uses Sieve theoretic methods

Theorem 37.0.8 (PNT for Dirichlet characters)**.**
There exists a $c_1 \geq 0$ such that for all $q \leq \exp(c_1\sqrt{\log x})$, we have

$$\psi(x,\chi) = \sum_{n\leq x}\Lambda(n)\chi(n) = \begin{cases} E_0(x) + \mathcal{O}(x\exp(-c_1\sqrt{\log x})) & \chi \text{ has no Siegel zero} \\ -\frac{x^{\beta_1}}{\beta_1} + \mathcal{O}(x\exp(-c_1\sqrt{\log x})) & \chi \text{ has Siegel zero} \end{cases}$$

Here, $E_0(\chi) = 1$ if $\chi = \chi_0$ and 0 otherwise.

Recall from MA317 that $L(x,\chi) \neq 0$ when $\sigma \geq 1 - \frac{c}{\log q\tau}$ for some constant $c > 0$ with the exception of atmost one real zero (β_1 the Siegel zero)

Proposition 37.0.9.
Let c be as above and assume that $\sigma \geq 1 - \frac{c}{2\log q\tau}$. Then,

1. If $L(s,\chi)$ has no Siegel zero or if β_1 is a Siegel zero (thus χ quadratic) but $|s-\beta_1| \geq \frac{1}{\log q}$, then
$$\frac{L'}{L}(s,\chi) \ll \log q\tau$$
$$|\log L(s,\chi)| \ll \log\log q\tau + \mathcal{O}(1)$$
$$\frac{1}{L(s,\chi)} \ll \log q\tau$$
2. If β_1 is a Siegel zero and $|s-\beta_1| \leq \frac{1}{\log q}$, then
$$\frac{L'}{L}(s,\chi) = \frac{1}{s-\beta_1} + \mathcal{O}(\log q)$$

$$|\arg L(s,\chi)| \leq \log\log q + \mathcal{O}(1)$$
$$|s-\beta_1| \ll |L(s,\chi)| \ll |s-\beta_1|(\log q)^2$$

Part VI.

Commutative Algebra