[redacted]

SEMESTER NOTES

Irish Debbarma

Department of Mathematics
Indian Institute of Science, Bangalore

December 2022

Contents

Part I.

Modular Forms

l. Lecture-l:

2. Lecture-2:

3. Lecture-3 (10 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 $1 \le j \le m$.
  From the previous theorem we get $f \equiv 0$ and this implies $\{f_i\}$ is linearly independent and thus $\dim_{\mathbb{C}} M_k(\Gamma_1) \le m$.
  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

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

is a group homomorphism.

Definition 4.2.2.

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

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

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

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

Part II.

Elliptic Curves

5. Lecture-1:

6. Lecture-2:

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

7.1. Projective varieties

Definition 7.1.1.
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 7.1.2.
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 7.1.3.
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 7.1.4.
An ideal $I \subseteq \bar{k}[X_0, \ldots, X_n]$ is called a homogenous ideal if it is generated by homogenous polynomial.

Definition 7.1.5.
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 7.1.6.

- 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 7.1.7.
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 7.1.8.
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 7.1.9.
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 7.1.10.
$V \subseteq \mathbb{P}^2$ 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 7.1.11.
$V : 3X^3 + 4Y^3 + 5Z^3 = 0$. $V(\mathbb{Q}) = \emptyset$ but for all prime p we have $V(\mathbb{Q}_p) \neq \emptyset$

Definition 7.1.12.
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 7.1.13.
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 7.1.14.
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 7.1.15.
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 7.1.16.
$V : Y^2 = X^3 + 17 \subseteq \mathbb{A}^2 \to \mathbb{P}^2$ with $(X, Y) \mapsto [X : Y : 1]$. Here, $\overline{V} : Y^2Z = X^3 + 17Z^3$ and $\overline{V} \backslash V = \{[0 : 1 : 0]\}$

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

Part III.

Basic Algebraic Geometry

9. Lecture-l:

10. Lecture-2 (10 January, 2023):

10.1. 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 $xy \in IJ \subseteq \mathfrak{p}$.
- $\mathfrak{p} \supseteq I \cap J \Leftrightarrow IJ \subseteq \mathfrak{p}$.

10.2. Zariski topology

Definition 10.2.1.
- 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 10.2.2 (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 10.2.3.
$\mathrm{Spec}(R)$ 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 10.2.4.
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.

f is nilpotent from the result proven below. □

Definition 10.2.5.
$x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$.

Remark 10.2.6.
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

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

Proposition 10.2.7.

$$\bigcap_{\mathfrak{p} \supseteq J} \mathfrak{p} \subseteq \mathrm{Nil}(R)$$

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. □

ll. Lecture-3 (l2th January):

Part IV.

Algebraic Geometry I

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

12.1. Topological properties

Consider a topological space X.

Definition 12.1.1.
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 12.1.2. *Composition of quasi-compact maps is quasi-compact.*

Lemma 12.1.3.
X quasi-compact and $Y \subseteq X$ is closed implies Y is quasi-compact.

Proof. □

Proposition 12.1.4.
If X is quasi-compact and Hausdorff, then $E \subseteq X$ is quasi-compact iff E is closed.

Proof. □

Lemma 12.1.5.
Any finite union of quasi-compact spaces is quasi-compact.

Proof. □

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

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

is stationary.

Lemma 12.1.6.
The following are equivalent:

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

Definition 12.1.7.
A topological space is called Noetherian if set of all closed subsets of X satisfies dcc.

Lemma 12.1.8.
X Noetherian implies X is quasi-compact.

Lemma 12.1.9.
If $X_1, \ldots, X_n$ are Noetherian subspaces of X, then so is $X_1 \cup X_2 \cup \ldots \cup X_n$

Lemma 12.1.10.
Quasi-compact and locally Noetherian implies Noetherian.

Exercise 12.1.11. *Give an example of a ring R such that $\mathrm{Spec}(R)$ is Noetherian but R is not.*

Definition 12.1.12.
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 12.1.13.
If X is Noetherian and $Y \subseteq X$ is a subspace, then Y is Noetherian.

Lemma 12.1.14.
Let X be Noetherian. Then, X has finitely many irreducible components.

Lemma 12.1.15.
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.

Lemma 12.1.16.
Suppose X is Noetherian and $X_1 \subseteq X$ an irreducible component. Then, X_1 contains a non-empty open set in X.

Definition 12.1.17.
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 $\overline{\{x\}} = X$)

12.2. 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 12.2.1.
$\mathrm{Spec}(A)$ is always spectral.

Proof. 1. X is T_0

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 $f_i s$.
   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 $\mathrm{Spec}(A) = \mathrm{Spec}(A_{\mathrm{red}}) = \mathrm{Spec}(A/\mathrm{Nil}(A))$.

□

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

13.1. Zariski topology contd..

Theorem 13.1.1 (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 13.1.2.
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 $f_{\#}(\mathfrak{p}) = f^{-1}(\mathfrak{p})$. We claim that $f_{\#}$ is continuous. This can be seen as follows: Take a basic open set $U = \mathrm{Spec}(A_a)$ and $b = f(a)$. Then, it is easy to see that $f_{\#}^{-1}(U_b) = U_a$. □

13.2. Affine schemes

Definition 13.2.1.
$\mathrm{Spec}(A)$ will be called an affine "scheme" (we will see this properly later on).

Definition 13.2.2.
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 13.2.3.
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 13.2.4.
If $X = \mathrm{Spec}(A)$. A regular function on X is a regular map from X to $\mathrm{Spec}(\mathbb{Z}[t])$.

Remark 13.2.5.
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 13.2.6.
Every affine scheme has a closed point.

Proof. Every commutative ring has a maximal ideal. □

Definition 13.2.7.
Open in affine is called quasi-affine.

Example 13.2.8.
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 $a_i = 0$

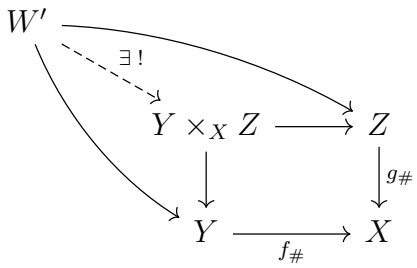
Exercise 13.2.9. *Let $A = k[X_1, X_2, \ldots], B = A_{\mathfrak{m}}, X = \mathrm{Spec}(B) \backslash \mathfrak{m}, \mathfrak{m} = \langle X_1, X_2, \ldots, \rangle$. Claim is that X has no closed point.*

13.2.1. 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 13.2.10.
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 13.2.11.
$\mathbf{Aff}_{\mathbb{Z}}$ = category of affine schemes admits fiber products.

Proof. Consider the following data:

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

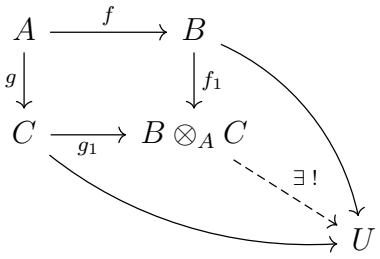
Let $D = B \otimes_A C$. We have the natural maps $f_1 : B \to B \otimes B \otimes C$ sending $b \mapsto b \otimes 1$ and $f_2 : C \to B \otimes C$ sending $c \mapsto 1 \otimes c$. Both are ring homomorphisms and fit into the following diagram due to the nature of tensor product

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

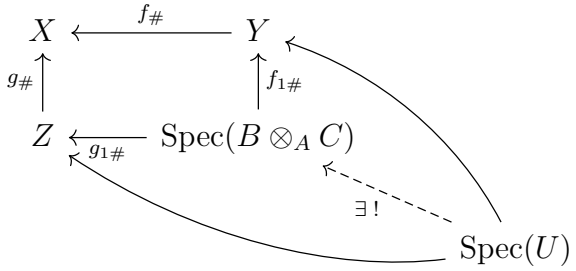
Now, let $W = \mathrm{Spec}(B \otimes_A C)$ and we claim that this satisfies the universal property of fibre product. Apply $\mathrm{Spec}(-)$ functor to the diagram to get

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

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



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



This completes the proof. □

14. Lecture-3:

Part V.

Topics in Analytic Number Theory

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

16. Lecture-2:

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

Theorem 17.0.1 (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 17.0.2.
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 17.0.3.

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

Theorem 17.0.4 (Y. Zhang)**.**

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

Theorem 17.0.5.
If $\chi(q)$ does not have a Siegel zero, then $L(1,\chi) \gg \frac{1}{\log q}$

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