[redacted]

SEMESTER NOTES

Irish Debbarma

Department of Mathematics
Indian Institute of Science, Bangalore

December 2022

Overview

These notes probably contain all the basics you will need in number theory. The Elliptic Curves book follows Silverman's Arithmetic of Elliptic Curves, Modular Forms follows Diamond Shurman's A first course in modular forms (it will contain a lot of theory of Riemann surfaces if I manage to do it ofc), Algebraic Geometry I covers range of topics, Basic Algebraic Geometry covers Fulton's Algebraic Curves. On top on that, I am also working to include relevant Commutative algebra, Algebraic Number Theory, Representation theory, Galois theory (finite and infinite).

I am trying to make it self contained and accessible to undergraduates, thus whenever you see interlude: it just means it was not covered in class but filled in by me later on to cover the gap of knowledge I had.

I will also try to mention external resources used so that original material is kept on record and properly referenced.

This section is just a reminder to myself on how to organise and stuff. So, feel free to ignore this part.

Contents

Part I.

Modular Forms

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

2. Lecture-2 (5th January, 2023): Modular Group and Binary quadratic forms

2.1. Modular Group and Upper Half Plane

The modular group is the group of 2×2 matrices with integer entries and determinant 1,

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\} \tag{2.1}$$

Proposition 2.1.1 (DS, exercise 1.1.1)**.**
The modular group $\mathrm{SL}_2(\mathbb{Z})$ is generated by $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Proof. Let Γ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by S, T. Observe that

$$S^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{ for } n \in \mathbb{Z} \tag{2.2}$$

Next, take an element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then,

$$\begin{aligned} \gamma S^n &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a & an + b =: b' \\ c & nc + d =: d' \end{pmatrix} \\ \gamma T &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} b & -a \\ d & -c \end{pmatrix} \end{aligned}$$

Suppose $c \neq 0$. If $|d| \geq |c|$, then we can employ Euclidean algorithm to get $d = cq + r$ with $0 \leq r < |c|$. If we perform γS^{-q}, then d' in the following matrix has the value $r < |c|$.

Now, apply T to switch (c, r) to $(r, -c)$ and now we have $|c| > r$ and we can continue the process. Finally after multiplying by S^α's and T's we get $\gamma\gamma_1 \in \mathrm{SL}_2(\mathbb{Z})$ with the last

row $(0, *)$.

This matrix is integral with determinant 1. Therefore it has the form $\begin{pmatrix} \pm 1 & m \\ 0 & \pm 1 \end{pmatrix}, m \in \mathbb{Z}$. Therefore, the final form is either S^m or S^{-m}. Hence, there exists a $\gamma_1 \in \Gamma$ such that $\gamma\gamma_1 \in \Gamma \ \forall \ \gamma \in \mathrm{SL}_2(\mathbb{Z})$. We can thus conclude that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Thus, Γ is the entire group. □

An element of the modular group can also be viewed as an automorphism of the Riemann surface $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ through the fractional linear transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \cdot z = \frac{az+b}{cz+d}, z \in \widehat{\mathbb{C}} \tag{2.3}$$

If $c \neq 0$, then $-d/c$ maps to ∞ and ∞ maps to a/c. If $c = 0$, then ∞ maps to ∞.

We also note that I and $-I$ give the identity transformation. Moreover, each pair $\pm\gamma$ give the same transformation. The group of transformations of the modular group is determined by the transformations carried out by its generators S, T as

$$z \mapsto z + 1, \quad z \mapsto -1/z$$

Proposition 2.1.2 (DS, Exercise 1.1.2)**.**

1. $\mathrm{Im}(\gamma(z)) = \mathrm{Im}(z)/|cz+d|^2$ for all $\gamma \in \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$
2. $(\gamma\gamma')(z) = \gamma(\gamma'(z)) \ \forall \ \gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z}), z \in \mathcal{H}$
3. $d\gamma(z)/dz = 1/(cz+d)^2$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$

Proof. 1. Observe that

$$\begin{aligned} \gamma \cdot z &= \frac{az+b}{cz+d} \\ \mathrm{Im}(\gamma \cdot z) &= \frac{1}{|cz+d|^2}\mathrm{Im}(adz + bc\bar{z}) \\ &= \frac{1}{|cz+d|^2}(ad(x+iy) + bc(x-iy)) \\ &= \frac{\mathrm{Im}(z)}{|cz+d|^2} \end{aligned}$$

2.

$$\begin{aligned}
\gamma\gamma' &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \\
\gamma' \cdot z &= \frac{a'z + b'}{c'z + d} \\
\gamma(\gamma'(z)) &= \gamma \cdot \frac{a'z + b'}{c'z + d} \\
&= \frac{aa'z + ab' + bc'z + bd'}{ca'z + b'c + c'dz + dd'}
\end{aligned}$$

3.

$$\begin{aligned}
\frac{d}{dz}\gamma(z) &= \frac{d}{dz}\left(\frac{az + b}{cz + d}\right) \\
&= \frac{a}{cz + d} - \frac{(az + b)c}{(cz + d)^2} \\
&= \frac{acz + ad - acz - bc}{(cz + d)^2} \\
&= \frac{1}{(cz + d)^2}
\end{aligned}$$

□

Definition 2.1.3.
Let k be an integer. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is a weakly modular of weight k if

$$f(\gamma(z)) = (cz + d)^k f(z) \quad \text{for} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{and } z \in \mathcal{H}$$

Remark 2.1.4.
Since $\mathrm{SL}_2(\mathbb{Z})$ is generated by S, T, we just need to check the invariance under the action of these two matrices, i.e., that

$$f(z + 1) = f(z) \quad \text{and} \quad f(-1/z) = z^k f(z)$$

for all $z \in \mathcal{H}$

Lemma 2.1.5.
There are no non-zero weakly modular functions of odd weights.

Proof. Let k be odd and f be a weakly modular function of weight k. Therefore, $f(-I \cdot z) = (-1)^k f(z)\ \forall\ z \in \mathcal{H}$ and thus $f(z) = 0\ \forall\ z \in \mathcal{H}$. □

Remark 2.1.6.
Suppose we want a function that is holomorphic on the upper half plane $\mathcal{H}$ and ∞. Note that $\mathrm{SL}_2(\mathbb{Z})$ contains the translation matrix $S : z \mapsto z+1$, so that $f(z+1) = f(z)$ for every weakly modular function $f : \mathcal{H} \to \mathbb{C}$. That is to say that f is $\mathbb{Z}$-periodic. Let D' be the open complex unit disc punctured at the origin. We know that $\mathbb{Z}$-periodic holomorphic map $z \mapsto \exp(2\pi i z) = q$ that takes $\mathcal{H}$ to D'. Thus, corresponding to f we have a function $g : D' \to \mathbb{C}$ such that $g(q) = f(\log(q)/(2\pi i))$. Then, g is well-defined even though log is defined only upto $2\pi i\mathbb{Z}$ and $f(z) = g(\exp(2\pi i z))$. If f is holomorphic on the upper half plane, then g is holomorphic on the punctured disc as the log is defined holomorphically around each point and thus g has a Laurent series expansion $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n, q \in D'$. The relation $|q| = \exp(2\pi \mathrm{Im}(z))$ shows that $q \to 0$ if $\mathrm{Im}(z) \to \infty$. So, thinking of ∞ as lying far in the imaginary direction, we define f to be holomorphic at ∞ if g extends to a holomorphic function at $q = 0$, i.e., the Laurent series sums over $\mathbb{N}$. This means that f has the Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, q = \exp(2\pi i z)$$

Since $q = 0$ iff $\mathrm{Im}(z) \to \infty$, showing that to check if a weakly holomorphic function is holomorphic at ∞ we just need to check whether $\lim_{\mathrm{Im}(z)\to\infty} f(z)$ exists or even bounded works.

Definition 2.1.7.
Let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k if

1. f is holomorphic on $\mathcal{H}$
2. f is weakly modular of weight k
3. f is holomorphic at ∞

   If in addition, we have

4. $a_0 = 0$ in the Fourier expansion of f, then we say f is a cusp form of weight k

We denote the space of modular forms of weight k by $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and the space of cusp forms of weight k by $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Proposition 2.1.8 (DS, Exercise 1.1.3)**.**

1. $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a vector space over $\mathbb{C}$
2. If f is a modular form of weight k and g a modular form of weight ℓ, then fg is a modular form of weight $k\ell$
3. $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is a vector subspace of $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and further, $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ is

an ideal of $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$

Proof. Really not in a mood. Someday □

Remark 2.1.9.
The second property in previous proposition gives the space $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ a graded structure, therefore

$$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$$

Similarly, using part 3 of the previous theorem and the above observation, we also have

$$\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$$

2.2. Fundamental domain

Definition 2.2.1.
Let Γ be a group acting on $\mathcal{H}$. A fundamental domain of Γ is a closed subset $\mathcal{D} \subseteq \mathcal{H}$ such that

1. The set $\mathcal{D}$ is the closure of its interior.
2. Every point in $\mathcal{H}$ is Γ equivalent to a point in $\mathcal{D}$.
3. If $z, w \in \mathcal{D}$ are Γ equivalent, then they lie on the boundary of $\mathcal{D}$.

Proposition 2.2.2.
The set

$$\mathcal{F}_1 = \{z \in \mathcal{H} : |z| > 1, |\Re z| < 1/2\}$$

is a fundamental domain of the full modular group Γ_1/

Proof. □

2.3. Binary Quadratic Forms

2.4. Compactification of $\mathrm{SL}_2(\mathbb{Z})$ and cusps

We can compactify $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ by adding a cusp at ∞.

$$\begin{aligned} \mathcal{H} &\to D' \\ z &\mapsto q = \exp(2\pi i z) \end{aligned}$$

Adding a cusp at ∞ is the same as adding $q = 0$. $\overline{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \cup \{\infty\}$.

The open neighbourhoods of ∞ are

$$U_y = \{z \in \mathcal{H} : \Im(z) > y\}$$

with $y > 1$. In the disc D', U_y goes to $\{0 < q < \exp(-2\pi y)\}$

Definition 2.4.1.
We will call $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ the projective rational line. The action of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is given by the usual fractional transformation

$$\gamma \cdot z = \frac{az + b}{cz + d}$$

Here, $\gamma \cdot \infty = a/c$ and $\gamma \cdot z = \infty$ if $cz + d = 0$

Exercise 2.4.2. *The two ways to compactify are the same.*

Proposition 2.4.3.
The action of $\mathrm{SL}_2(\mathbb{Z})$ is transitive on $\mathbb{P}^1(\mathbb{Q})$

Proof. Take an element $t \in \mathbb{Q}$. Write $t = a/c$ in the reduced form, then there exists integers b, d such that $ad - bc = 1$. Therefore, we have $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Clearly, $\gamma \cdot \infty = t$. □

Remark 2.4.4.
Note that $\mathrm{SL}_2(\mathbb{Z})_\infty = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \frac{a}{c} = \infty\} = \{\pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}\}$
Therefore, there is a bijection

$$\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})_\infty \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q})$$

We want to study stabilisers of each point of $\overline{\mathcal{F}}_1$. Let $z \in \overline{\mathcal{F}}_1$ and $\mathrm{SL}_2(\mathbb{Z}) \ni \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

We want to examine

$$\begin{aligned} \gamma \cdot z &= z \\ \frac{az + b}{cz + d} &= z \\ cz^2 + (d - a)z - b &= 0 \end{aligned}$$

Since $c \neq 0, z \notin \mathbb{Q}$, therefore the discriminant must be negative or $(a + d)^2 - 4 < 0 \Rightarrow |a + d| < 2$

Exercise 2.4.5. *γ satisfies $X^2 + 1 = 0$ or $X^2 \pm X + 1 = 0$.*

Proposition 2.4.6. 1. If $z \in \mathcal{F}_1$, then $\mathrm{Stab}(z) = \{\pm \mathrm{Id}_2\}$

2. If $z = \exp(2\pi i/3) =: \omega$, then $\mathrm{Stab}(\omega) = \langle \pm ST \rangle$.

3. If $z = i$, then $\mathrm{Stab}(i) = \langle \pm S \rangle$

If k is even, then $-\mathbf{Id}_2$ acts as identity on a modular form of weight k. Let $P \in \overline{\mathcal{F}}_1$. We define

$$n_P = \begin{cases} 1 & , P \not\sim i, \omega \\ 2 & , P \sim i \\ 3 & , P \sim \omega \end{cases}$$

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

3.1. Valence formula

Definition 3.1.1.
Let $0 \neq f : \mathcal{H} \to \mathbb{C}$ be a meromorphic function and $P \in \mathcal{H}$. The smallest integer n such that $(z-P)^{-n} f(z)$ is holomorphic and non-vanishing at P is called the order of f at P, denoted by $\mathrm{ord}_P(f)$. We say that f has a zero of order n if n is positive and pole of order n if n is negative.

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 3.1.2.
$$\dim \mathcal{M}_k(\Gamma_1) = \begin{cases} [k/12]+1 & k \not\equiv 2 \pmod{12} \\ [k/12] & k \equiv 2 \pmod{12} \end{cases}$$

Lemma 3.1.3.
Let $0 \neq f$ be a modular function. Then there exists a $R < \infty$ such that f is holomorphic and non-vanishing on $\Im z > R$

Proof. Since f is holomorphic at ∞ therefore g is holomorphic in the region $\{z \in \mathbb{C} : 0 < |z| < R''\}$ for some $R > 0$. Since f is non-zero, therefore g is also non-zero and cannot be an accumulation point of zeroes of g. Thus, there exists $R' > 0$ such that g is non-zero and holomorphic in the region $\{z \in \mathbb{C} : 0 < |z| < R'\}$. This implies $f = g \circ q$ is holomorphic and non-zero in $\mathcal{H}$ if $|q(z)| < R' \Leftrightarrow |\exp(2\pi i z)| < R' \Leftrightarrow \exp(-2\pi \Im z) < R' \Leftrightarrow -2\pi \Im z < \log R' \Leftrightarrow \Im z > \frac{1}{2\pi} \log(1/R') := R$ □

Proposition 3.1.4.
Let $f \in \mathcal{M}_k(\Gamma_1)$. Then,
$$\sum_{p \in \Gamma_1 \backslash \mathcal{H}, p \neq i, \omega} \mathrm{ord}_p(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\omega(f) + \mathrm{ord}_\infty(f) = \frac{k}{12}$$

Or, more generally

$$\sum_{P\in\Gamma_1\backslash\mathcal{H}} \frac{1}{n_P}\mathrm{ord}_P(f) + \mathrm{ord}_\infty(f) = \frac{k}{12}$$

Proof. Consider the contour $\mathcal{C}$ as follows:
We just consider the case where $\mathcal{F}_1$ contains all its zeroes and poles inside the contour and □

Corollary 3.1.5.

$$\dim \mathcal{M}_k(\Gamma_1) = \begin{cases} 0 & k < 0 \\ 0 & k \text{ is odd} \\ 1 & k = 0 \\ \begin{cases} [k/12]+1 & k \not\equiv 2 \pmod{12} \\ [k/12] & k \equiv 2 \pmod{12} \end{cases} \end{cases}$$

Proof.

- If $k < 0$, then LHS is > 0 but RHS is < 0. A contradiction.
- We have already seen
- For $k = 0$, take $f \in \mathcal{M}_0(\Gamma_1)$. Clearly, $\mathcal{M}_0(\Gamma_1) \ni f(\infty) = c \Rightarrow f - c \in \mathcal{M}_0(\Gamma_1)$. Since, the LHS is > 0 and RHS $\equiv 0$ therefore $f \equiv c$.
- Let $m = [k/12] + 1$ and take $f_1, \ldots, f_{m+1} \in \mathcal{M}_k(\Gamma_1)$. If $P_1, \ldots, P_m$ are points in $\mathcal{F}_1$ not equal to $i, \omega, \omega + 1$ and consider $\{f_i(P_j)\}_{1\le i\le m+1, 1\le j\le m}$.
  Next, consider the linear combination $f = \sum_{i=1}^{m+1} c_i f_i$ with not all c_is zero so that $f(P_j) = 0$ for $1 \le j \le m$. From the previous theorem, this means $f \equiv 0$ and hence $\{f_i\}$ is linearly independent and hence $\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma_1) \le m$.
  For $k \equiv 2 \pmod{12}$, the relation holds only if there is atleast a simple pole at i and a double zero at ω. Therefore,

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

  Therefore, we can repeat the argument.

□

Remark 3.1.6.
The above result only gives us an upper bound. To get lower bound, we will need a bit more machinery.

Theorem 3.1.7.
Let f be a modular form of weight k and level 1 with q-expansion $\sum_{n=1}^{\infty} a_n q^n$. Suppose

$$a_n = 0 \text{ for } n = 0, \ldots, [k/12]$$

then $f = 0$.

Proof. Suppose $f \neq 0$. By our assumption, $\mathrm{ord}_\infty(f) \geq [k/12] + 1 > k/12$. By the valence formula, the LHS $> k/12$ which is a contradiction. Therefore $f = 0$. □

Corollary 3.1.8.
Suppose f, g are modular forms of weight k, level 1 with q expansions $f(q) = \sum_{n=1}^{\infty} a_n q^n, g(q) = \sum_{n=1}^{\infty} b_n q^n$. If

$$a_n = b_n \quad \text{for } n = 0, \ldots, [k/12]$$

then $f = g$.

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.

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

Proof.

$$\begin{aligned} E_k(z) &= \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_1} 1|_\gamma(z) \\ &= \sum_{\gamma \in \overline{\Gamma}_\infty \backslash \overline{\Gamma_1}} 1|_\gamma(z) \end{aligned}$$

If $(c, d) = 1$ then there exists $a, b \in \mathbb{Z}$ such that $ad - bc = 1 \to \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.
And, conversely if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ then $(c, d) = 1$.

If $\begin{pmatrix} a' & b' \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then we want to show that there is an $\eta \in \Gamma_\infty$ such that $\eta \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) = \begin{pmatrix} a' & b' \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$

Note that $ad - bc = 1 = a'd - b'c \Rightarrow (a - a')d = (b - b')c \Rightarrow (a - a') = nc, b - b' = nd$. Thus, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' + nc & b' + nd \\ c & d \end{pmatrix} = S^n \begin{pmatrix} a' & b' \\ c & d \end{pmatrix}$ But, $T^n \in \Gamma_\infty$. This completes the proof. □

Proposition 3.2.3 (DS, Exercise 1.1.4)**.**

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

converges absolutely for $k > 2$

Proof.

- Consider the sum $\sum_{(a,b)\in\mathbb{Z}^2-\{(0,0)\}} \sup\{|a|,|b|\}^{-k}$. We shall prove that this sum converges.
  First, we can sum this over the first quadrant only and quadruple the value later. So, let us focus on
  $$\sum_{(a,b)\in\mathbb{Z}^2_{>0}-\{(0,0)\}} \sup\{|a|,|b|\}^{-k}$$
  Look at the partial sums:
  $$\sum_{(a,b)\in\mathbb{Z}^2_{>0,leN}-\{(0,0)\}} \sup\{|a|,|b|\}^{-k} \leq \sum N^{-k} = \frac{N^2-1}{N^k}$$

- Next, consider $\Omega = \{\tau \in \mathcal{H} : |\Re\tau| \leq A, \Im\tau \geq B\}$.
  Claim: $\exists c > 0$ such that $|\tau + \delta| > C \sup\{1, |\delta|\}$

  Proof. For $|\delta| < 1$, $|\tau + \delta| > |\tau| > \Im\tau \geq B$.
  For $|\delta| > 2A$, $|\tau + \delta| > |\Re\tau + \delta| \geq |\delta| - |\Re\tau| \geq \delta - A \Rightarrow |\tau + \delta| \geq |\delta| - A > |\delta|/2 = 1/2 \sup\{1, |\delta|\}$. Therefore $C = \min\{1/2, B\}$ works.
  For $1 < |\delta| < 2A$ and $\Im\tau \geq A$, $|\tau + \delta| > A > |\delta|/2$
  For $1 < |\delta| < 2A$ and $B \leq \Im\tau \geq A$, $|\tau + \delta|/|\delta|$ has a minimum m. Therefore, $|\tau + \delta| \geq m|\delta|$. □

- Now, using the above two observations, we have

$$\begin{aligned} E_k(\tau) &= \sum{}' \frac{1}{(c\tau+d)^k} \\ &= \sum_d \frac{1}{d^k} + \sum_{c\neq 0,d} \frac{1}{(c\tau+d)^k} \\ &= 2\zeta(k) + \sum_{c\neq 0,d} \frac{1}{(c\tau+d)^k} \end{aligned}$$

Now, $|c\tau+d| = |c||\tau+\delta| > |c|C_1 \sup\{1,|\delta|\}$

$$\therefore \frac{1}{C_1^k} \sum_{c\neq 0,d} \frac{1}{(|c|^k \sup\{1,|\delta|\}^k}$$

converges for $\tau \in \Omega$ and since any compact set in $\mathcal{H}$ sits inside a suitable Ω, our claim is proven.

□

Theorem 3.2.4 (DS, Exercise 1.1.4)**.**
$E_k(z) \in \mathcal{M}_k(\Gamma_1)$ for $k > 2$.

Proof. Clearly, $E_k(\tau+1) = E_k(\tau)$ and $E_k(-1/\tau) = \tau^k E_k(\tau)$. Therefore, it is weakly modular of weight k and level 1. Previous proposition says that it is holomorphic on $\mathcal{H}$. We just need to check holomorphicity at ∞.
Let $\tau = i\nu$ and observe the sum as $\nu \to \infty$. Then, the sum is determined by the behaviour of $\sum_d d^{-k}$ and since $k \geq 3$, this sum is convergent and hence the sum is bounded and we are done. It is indeed a modular form of weight k and level 1. □

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

Proof. First of all notice that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(m,n) = (am+bn, cm+dn), a,b,c,d \in \mathbb{Z}$. Since the matrix is invertible, multiplication by $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is a bijection from $\mathbb{Z}^2 - \{(0,0)\}$ to $\mathbb{Z}^2 - \{(0,0)\}$.

Next, 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 $k > 2$.

Proof. Same as above. □

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

Proof.

$$\begin{aligned} G_k(z) &= \sum'_{(c,d)\in\mathbb{Z}^2} \frac{1}{(cz+d)^k} \\ &= \sum'_{(c,d)\in\mathbb{Z}^2,\gcd(c',d')=1} \frac{1}{\gcd(c,d)^k} \cdot \frac{1}{(c'z+d')^k} \\ &= \zeta(z)E_k(z) \end{aligned}$$

□

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

$$\mathcal{M}(\Gamma_1) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\Gamma_1)$$

is a graded ring.

Proposition 4.1.1.
The graded ring $\mathcal{M}(\Gamma_1)$ is freely generated by E_4, E_6. This means that the map

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

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. □

Corollary 4.1.2.

$$\dim_{\mathbb{C}} M_k(\Gamma_1) \geq \begin{cases} [k/12]+1 & k \not\equiv 2 \pmod{12} \\ [k/12] & k \equiv 2 \pmod{12} \end{cases}$$

Proof. By the previous proposition, $E_4^a E_6^b$ is a basis for the space of modular forms. Clearly, $\{E_4^a E_6^b : \mathbb{Z} \ni a, b, 4a+6b=k\}$ forms a basis for $\mathcal{M}_k(\Gamma_1)$. We just have to compute the size of this set. That is we want to find the size of the set $\{(a,b) \in \mathbb{Z}_{\geq 0} : 4a+6b=k\}$. Since k is also even, let us divide by 2 and reduce to the set $\{(a,b) \in \mathbb{Z}_{\geq 0} : 2a+3b=k\}$ with $k=6m+n$ and $k, n \in \{0,1,2,3,4,5\}$. We wish to show that

$$\#\{(a,b) \in \mathbb{Z}_{\geq 0} : 2a+3b=k\} = \begin{cases} m+1 & k \not\equiv 1 \pmod 6 \\ m & k \equiv 1 \pmod 6 \end{cases}$$

- $n=1$, then we have $2a = 6m + (1-3b) \geq 0 \Rightarrow 0 \leq b \leq 1/3 + 2m$. And, moreover b has to be odd and hence we have m choices.
- $n=0$, then we have $2a = 6m - 3b \geq 0 \Rightarrow 0 \leq b \leq 2m$ and b is even therefore $m+1$ choices.

Similarly for the others. □

This completes the proof of the theorem

Theorem 4.1.3.

$$\dim_{\mathbb{C}} M_k(\Gamma_1) = \begin{cases} [k/12]+1 & k \not\equiv 2 \pmod{12} \\ [k/12] & k \equiv 2 \pmod{12} \end{cases}$$

4.1.1. Fourier expansions of $E_k(z)$

Proposition 4.1.4 (DS, Exercise 1.1.7)**.**

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

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 4.1.5 (DS, Exercise 1.1.5)**.**

$$\begin{aligned}
\cot \pi\tau &= \frac{\cos \pi\tau}{\sin \pi\tau} \\
&= i\frac{e^{i\pi\tau} + e^{-i\pi\tau}}{e^{i\pi\tau} - e^{-i\pi\tau}} \\
&= i\frac{q+1}{q-1} \\
&= i + i\frac{2}{q-1} \\
&= i - 2i\sum_{m=0}^{\infty} q^m \\
\therefore \pi \cot \pi\tau &= \pi i - 2\pi i \sum_{m=0}^{\infty} q^m
\end{aligned}$$

And,

$$\begin{aligned}
\sin \pi\tau &= \pi\tau \prod_{j=1}^{\infty}\left(1 - \frac{\tau^2}{j^2}\right) \\
\log \sin \pi\tau &= \log \pi\tau + \sum_{j=1}^{\infty} \log\left(1 - \frac{\tau^2}{j^2}\right) \\
\pi\frac{\cos \pi\tau}{\sin \pi\tau} &= \frac{1}{\tau} + \sum_{j=1}^{\infty} \frac{2\tau}{1 - \frac{\tau^2}{j^2}} \\
\pi \cot \pi\tau &= \frac{1}{\tau} + \sum_{j=1}^{\infty} \frac{\tau + j + \tau - j}{(\tau - j)(\tau + j)} \\
&= \frac{1}{\tau} + \sum_{d=1}^{\infty} \frac{1}{\tau + d} + \frac{1}{\tau - d}
\end{aligned}$$

Remark 4.1.6.

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 4.1.7 (DS, Exercise 1.1.7)**.**

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

Proof. Look at the space $\mathcal{M}_8(\Gamma_1)$. This is 1-dimensional. Therefore, E_4^2 and E_8 by virtue of being modular forms of weight 8 must be linearly dependent. Thus, $E_8(\tau) = \lambda E_4^2(\tau)$.

But, both have the same constant term and hence equal. After that, it is just comparing coefficients of the Fourier expansion. □

4.1.2. Weight 2 Eisenstein series

Definition 4.1.8.

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

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

Proposition 4.1.9.

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

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.

Lemma 4.1.10.

Proof. □

□

Proposition 4.1.11.
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 (DS, Exercise 1.2.2)**.**
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.

- $\gcd(c, d, N) = 1$. Indeed, if $\gcd(c, d, N) = g$, then $g \mid (ad - bc) = 1 \Rightarrow g \mid 1 \Rightarrow g = 1$.
- Now, write $c = c_1c_2$ such that $\gcd(c, N) = c_2$. Then, $\gcd(c_1, N) = 1$. For, suppose if $p \mid N$, then $p \mid c_2$ necessarily. Now, there exists integers $r, s \in \mathbb{Z}$ such that $1 = c_1r + Ns \Rightarrow 1 \equiv Ns \pmod{c_1}$
- Let $c' = c$ and $d' = d + mN$ where $m = s(1 - d)$. Clearly, $d + mN \equiv 1 \pmod{c_1}$. We claim that $\gcd(c', d') = 1$. Indeed, if $p \mid c', d' \Rightarrow p \mid c, d + mN$. Since $c = c_1c_2$ we have $p \mid c_1$ or $p \mid c_2$. If $p \mid c_1$, then we get a contradiction to $d + mN \equiv 1 \pmod{c_1}$. Hence, $p \mid c_2$ which then implies that $p \mid N \Rightarrow p \mid \gcd(c, d, N)$ a contradiction.
- Now, we can lift γ to $\begin{pmatrix} a + kN & b + lN \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$

Finally, we can conclude that this map is surjective. □

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

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

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

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 $\mathcal{H}$.

Proof. From the valence formula we have

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

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

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, $f(z) - a_0 E_4^a(z)E_6^b(z) \in \mathcal{M}_k(\Gamma_1) \subseteq \mathcal{S}_k(\Gamma_1)$.
Next,

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

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

Proposition 5.1.3.

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

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

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 $\Gamma_1 \backslash \bar{\mathcal{H}}$. □

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 $691 \mid \#\mathcal{C}(\mathbb{Q}(\gamma_{691}))$)

5.2. Congruence subgroup

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

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

Proof. By CRT, we have $\mathbb{Z}/N\mathbb{Z} = \prod_{i=1}^{r} \mathbb{Z}/p^{a_i}\mathbb{Z}$. This completes the proof. □

Lemma 5.2.2 (DS, Exercise 1.2.3)**.**

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

Proof.

- First, we need to find $\#\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$. We will prove $\#\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}) = p^{3e}(1 - 1/p^2)$ by induction.
- $n = 1 \Rightarrow \#\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = p^3(1 - 1/p^2) = p(p^2 - 1)$
- Suppose assertion is true for $n = k - 1$
- The map $\mathrm{SL}_2(\mathbb{Z}/p^k\mathbb{Z}) \xrightarrow{\phi} \mathrm{SL}_2(\mathbb{Z}/p^{k-1}\mathbb{Z})$ be the surjective reduction map.
- The kernel of ϕ is $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^k\mathbb{Z}) : a, d \equiv 1 \pmod{p^{k-1}}, b, c \equiv 0 \pmod{p^{k-1}}\}$
- Let $a = up^{k-1} + 1, b = vp^{k-1} + 1, c = rp^{n-1}, d = sp^{k-1}$
- Then,

$$\begin{aligned} ad - bc &= usp^{2k-2} + up^{k-1} + sp^{k-1} + 1 - vrp^{2k-2} \\ &\equiv (u+s)p^{k-1} + 1 \pmod{p^k} \\ &\equiv 1 \pmod{p^k} \\ (u+s)p^{k-1} &\equiv 0 \pmod{p^k} \end{aligned}$$

  This means $p \mid u + s$

- Now, (u, s) can be chosen in p many ways and v, r can be chosen in p^2 many ways.
- To conclude, $\#\mathrm{SL}_2(\mathbb{Z}/p^k\mathbb{Z}) = p^3 p^{3(k-1)-2}(p^2 - 1) = p^{3k-2}(p^2 - 1)$
- Now, using the previous proposition we can conclude what we want.

□

Remark 5.2.3 (DS, Exercise 1.2.3)**.**

1. Consider the map $\Gamma_1(N) \xrightarrow{\phi} \mathbb{Z}/N\mathbb{Z}$ given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \pmod N$. This map clearly surjects and the kernel is $\Gamma(N)$
2. The map $\Gamma_0(N) \xrightarrow{\phi} (\mathbb{Z}/N\mathbb{Z})^\times$ given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \pmod N$ surjects and has $\Gamma_1(N)$ as kernel.
3. Now, using the previous lemma and the above two remarks we have

$$\begin{aligned}
[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] &= \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma_0(N) : \Gamma_1(N)][\Gamma_1(N) : \Gamma(N)]} \\
&= \frac{N^3 \prod_{p|N}(1 - 1/p^2)}{N \cdot \varphi(N)} \\
&= \frac{N^3 \prod_{p|N}(1 - 1/p^2)}{N \cdot N \prod_{p|N}(1 - 1/p)} \\
&= N \prod_{p|N}(1 + 1/p)
\end{aligned}$$

Definition 5.2.4.
A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is called congruence subgroups if $\Gamma(N) \subseteq \Gamma$ for some $N \geq 1$.

Lemma 5.2.5.
A congruence subgroup has finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Proof. By definition $\Gamma(N) \subseteq \Gamma$ for some $N \geq 1$. This implies $\#(\mathrm{SL}_2(\mathbb{Z})/\Gamma) \leq \#(\mathrm{SL}_2(\mathbb{Z})/\Gamma(N))$ But the RHS is exactly $\#(\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ which is finite. This completes the proof. □

Remark 5.2.6.
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 5.2.7.
Γ is the smallest index subgroup that is non-congruence.

Definition 5.2.8.
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 $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$.

5.3. Fundamental Domain

6. Lecture-6 (19th January, 2023): Cusps, congruence modular forms and enhanced elliptic curves

6.1. Cusps

Suppose p is a prime.

Proposition 6.1.1.

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

Proposition 6.1.2.

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

Proof. Take an element $t \in \mathbb{Q}$. Write $t = a/c$ in the reduced form, then there exists integers b, d such that $ad - bc = 1$. Therefore, we have $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$. Clearly, $\gamma \cdot \infty = t$. We now consider two cases:

- If $p \mid c$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p) \Rightarrow a/c \in [\infty]$. Conversely, if $\gamma \in \Gamma_0(p)$, then p divides the denominator of $\gamma \cdot \infty$. Therefore $[\infty]$ is given by all rationals a/c such that $p \mid c$
- If $p \nmid c$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$, then $p \nmid d$ since $ad - bc = 1$. Therefore, p cannot divide the denominator of $\gamma \cdot 0$. Conversely, if b/d is such that $\gcd(b, d) = 1, p \nmid d$. Then, $\exists a, c$ such that $ad - bc = 1$. We can replace c with $c' = c + \lambda d, a' = a + \lambda d$ for some integer λ such that $c' \equiv 0 \pmod{p}$. Then, $\begin{pmatrix} a' & b \\ c' & d \end{pmatrix} \in \Gamma_0(p)$.

□

Definition 6.1.3.
If Γ is a congruence subgroup. Then the cusps of Γ is the set of Γ orbits in $\mathbb{P}^1(\mathbb{Q})$, i.e.,

$$\text{Cusps}(\Gamma) = \Gamma\backslash\mathbb{P}^1(\mathbb{Q}) = \Gamma\backslash\text{SL}_2(\mathbb{Z})/\text{SL}_2(\mathbb{Z})_\infty$$

Therefore there is a surjective map

$$\Gamma\backslash \mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{Cusps}(\Gamma)$$

Proposition 6.1.4.
Let Γ be a congruence subgroup, then $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ is finite. (called the cusps of level Γ).

Proof. Since there exists $N \in \mathbb{N}$ such that $\Gamma(N) \subseteq \Gamma$, we can just work with $\Gamma = \Gamma(N)$. Note that $\mathrm{SL}_2(\mathbb{Z}) = \sqcup_i g_i\Gamma$.
For any rational $q \in \mathbb{P}^1(\mathbb{Q})$ we have a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $q = \gamma \cdot \infty$. And hence $\exists\, i$ such that $\gamma = g_i\gamma'$. Thus, $q =$
$gamma'(g_i\infty)$ OR equivalently q is Γ equivalent to some $g_i(\infty)$. This completes the proof since $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$. □

Exercise 6.1.5.

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

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

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

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

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

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

Definition 6.1.6.
Let Γ be a congruence subgroup and $k \in \mathbb{Z}$. A modular form of weight k and level Γ is a function $f : \mathcal{H} \to \mathbb{C}$ such that

1. f is holomorphic on $\mathcal{H}$.
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 ∞.

Example 6.1.7.
$\Gamma_1(p)$ has cusps $0, \infty$. We just need to check

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

Notation:

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

Definition 6.1.8.
$f \in \mathcal{M}_k(\Gamma)$ 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 $\mathcal{S}_k(\Gamma)$ we denote the space of all cusp forms of weight k and level Γ.

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

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

Now, let Γ be a congruence subgroup. Define:

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

These are called modular curves.

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

6.2. Interlude: Complex Tori and Elliptic curves

6.2.1. Complex Tori

Definition 6.2.1.
Take $\omega_1, \omega_2 \in \mathbb{C}$ linearly independent over $\mathbb{R}$. We also make a normalising convention that $\omega_1/\omega_2 \in \mathcal{H}$. Then, a lattice in $\mathbb{C}$ is a set

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$$

Lemma 6.2.2.
Consider the two lattices $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}, \Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ with $\omega_1/\omega_2, \omega_1'/\omega_2' \in \mathcal{H}$. Then, $\Lambda = \Lambda'$ iff

$$\begin{pmatrix}\omega_1' \\ \omega_2'\end{pmatrix} = \begin{pmatrix}a & b \\ c & d\end{pmatrix}\begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix} \text{ for some } \begin{pmatrix}a & b \\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Proof. $(' \Rightarrow')$
Since ω_1, ω_2 is a basis, therefore $\omega_1' = a\omega_1 + b\omega_2, \omega_2' = c\omega_1 + d\omega_2$. Similary, since ω_1', ω_2' is a basis, therefore $\omega_1 = u\omega_1 + v\omega_2, \omega_2 = w\omega_1 + x\omega_2'$. Hence,

$$\begin{pmatrix}u & v \\ w & x\end{pmatrix}\begin{pmatrix}a & b \\ c & d\end{pmatrix} = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix}$$

Therefore, the determinant of each matrix is 1 which proves this direction.

$(' \Leftarrow')$
The lattice Λ' consists of all linear combinations of the form

$$x(a\omega_1 + b\omega_2) + y(c\omega_1 + d\omega_2) = (xa + yc)\omega_1 + (bx + dy)\omega_2$$

Therefore $\Lambda' \subseteq \Lambda'$. And, for any $m\omega_1 + n\omega_2 \in \Lambda$ we can always find (x, y) such that

$$\begin{pmatrix}a & b \\ c & d\end{pmatrix}\begin{pmatrix}x \\ y\end{pmatrix} = \begin{pmatrix}m \\ n\end{pmatrix}$$

Thus, we can infer that $\Lambda \subseteq \Lambda'$. Hence, we conclude our proof. □

Definition 6.2.3.
The parallelogram with vertices $z_0, z_0 + \omega_1, z_0 + \omega_2, z_0 + \omega_1 + \omega_2$ is called the fundamental parallelogram.

Lemma 6.2.4.
Any holomorphic map between compact Riemann surfaces is either a surjection or a map to one point.

Proof. Suppose $f : X \to Y$ be a holomorphic map between two compact Riemann surfaces X, Y. Since f is continuous and X is compact, therefore $f(X)$ is compact as

well. Same for connected. Unless f is constant, it is open by Open mapping theorem. Thus, $f(X)$ is clopen, (connected + compact $\Rightarrow$ closed) and connected. Hence, it is either a single point or the entirety of Y. □

Proposition 6.2.5.
Suppose $\phi : C/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic map between complex tori. Then there exists complex numbers m, b with $m\Lambda \subseteq \Lambda'$ such that $\phi(z+\Lambda) = mz + b\Lambda'$. The map is invertible iff $m\Lambda = \Lambda'$.

Proof. □

Corollary 6.2.6.
Suppose $\phi : C/\Lambda \to \mathbb{C}/\Lambda'$ is a holomorphic map between complex tori with $\phi(z+\Lambda) = mz + b\Lambda', m\Lambda = \Lambda'$. TFAE:

1. ϕ is a group homomorphism.
2. $b \in \Lambda'$, so $\phi(z+\Lambda) = mz + \Lambda'$.
3. $\phi(0) = 0$

Proof. $1 \Rightarrow 3 \Rightarrow 2 \Rightarrow 1$ □

6.2.2. Complex Tori as elliptic curves

Definition 6.2.7.
Given a lattice Λ, we define the Weierstrass $\wp$-function as

$$\wp(z;\Lambda) = \frac{1}{\omega^2} + \sum_{\omega \in \Lambda - \{(0,0)\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{6.1}$$

$z \in \mathbb{C}, z \notin \Lambda$

Eisenstein series generalises to

$$G_k(\Lambda) = \sum_{\omega \in \Lambda - \{(0,0)\}} \frac{1}{\omega^k}, k > 2 \text{ even} \tag{6.2}$$

Theorem 6.2.8 (Sil, Exercise 6.2)**.**
For any lattice Λ, the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C}\backslash\Lambda$. The series defines a meromorphic function on $\mathbb{C}$ having double pole with residue 0 at each lattice point and no other poles.

Proof.

- Observe the absolute value of a summand

$$\left|\frac{1}{(z-\omega)}-\frac{1}{\omega^2}\right| = \frac{|z||2\omega - z|}{|\omega|^2|z-\omega|^2} \leq \frac{|z|(2|\omega|+|z|)}{|\omega|^2(|z|-|\omega|)^2}$$

  Suppose $|\omega| > 2|z|$, then by reverse triangle inequality $|\omega - z| > |\omega|/2$, and $2|\omega| + |z| < 5|\omega|/2$. Hence,

$$\left|\frac{1}{(z-\omega)}-\frac{1}{\omega^2}\right| < \frac{|z|(2|\omega|+|z|)}{|\omega|^2(|z|-|\omega|)^2} < 10\frac{|z|}{|\omega|^3}$$

  On a compact disc $|z| < R$ this bound becomes $10R/|\omega|^3$.

  Thus, to prove convergence of the original series, we just need to check convergence of $\sum_{\omega} \frac{1}{\omega^3}$

- **Claim**: $\#\{\omega \in \Lambda : |\omega| \leq R\} = \pi R^2/A(\Lambda) + \mathcal{O}(R)$ where $A(\Lambda)$ is the volume of fundamental parallelogram.
  Let ω_1, ω_2 be the basis of Λ. And say $c = \max\{|\omega_1+\omega_2|, |\omega_1-\omega_2|\}$. Also, assume $R > c$. We can move the fundamental parallelogram a bit so that there is only one lattice point inside each parallelogram. Say B_R is the disc of radius R and K_R the intersection of all parallelograms that intersect B_R. Clearly, $B_R \subseteq K_R \subseteq B_{R+c}$. Therefore, B_R contains atmost $\pi(R+c)^2/A(\Lambda)$ many lattice points. And, $B_{R-c} \subseteq K_{R-c} \subseteq B_R$ which implies there are atleast $\pi(R-c)^2/A(\Lambda)$ many lattice points in B_R. To summarise

$$\frac{\pi(R-c)^2}{A(\Lambda)} < \text{ lattice points } < \frac{\pi(R+c)^2}{A(\Lambda)}$$

  And hence we conclude what we want.

- We can conclude that there exists a constant $c = c(\Lambda)$ such that

$$\#\{\omega \in \Lambda : N \leq |\omega| < N+1\} < cN$$

- Thus,

$$\sum_{\omega\in\Lambda}\frac{1}{\omega^3} \leq \sum_{N=1}^{3}\frac{\#\{\omega \in \Lambda : N \leq |\omega| < N+1}{N^3} \leq \sum_{N}\frac{c}{N^2} < \infty$$

This concludes the proof. □

Proposition 6.2.9.
Let $\wp$ be the Weierstrass function wrt to lattice Λ.

1. The Laurent expansion of $\wp$ is

$$\wp(z) = \frac{1}{z^2} + \sum_{n \equiv 0 \pmod 2} (n+1) G_{n+2}(\Lambda) z^n \tag{6.3}$$

for all z such that $0 < |z| < \inf\{|\omega| : \omega \in \Lambda - \{(0,0)\}\}$

2. The functions $\wp, \wp'$ satisfy the relation

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) \tag{6.4}$$

where $g_2(\Lambda) = 60G_4(\Lambda), g_3(\Lambda) = 140G_6(\Lambda)$

3. Let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ and $\omega_3 = \omega_1 + \omega_2$. Then the cubic equation satisfied by $\wp, \wp'$, $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, is

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3)$$

where $e_i = \wp(\omega_i/2), i = 1, 2, 3$

Proof. 1. Observe

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1 - z/\omega)^2} - 1\right)$$

Since we took $|z| < \inf\{|\omega| : \omega \in \Lambda - \{(0,0)\}\} \Rightarrow |z/\omega| < 1$ and thus we can use binomial expansion to get

$$\begin{aligned}
\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)(z/\omega)^2 \\
\therefore \wp(z) &= \frac{1}{z^2} + \sum_{\omega}{}' \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n \sum_{\omega}{}' \frac{1}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n}(n+1)G_{n+2}(\Lambda)z^n
\end{aligned}$$

The interchange of sums can be done due to absolute convergence. The odd terms in the last sum vanish therefore we obtain what we want.

2.

$$\wp(z) = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \mathcal{O}(z^6)$$
$$\wp'(z) = \frac{-2}{z^3} + 6G_4(\Lambda)z + 20G_6(\Lambda)z^3 + \mathcal{O}(z^5)$$

After some laborious calculation, we note that $(\wp'(z))^2$ and $4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$ evaluate to $\mathcal{O}(z^2)$. Hence, as $z \to 0$ the difference of the two mentioned in the previous line goes to zero. Moreover, the difference is periodic, holomorphic and thus bounded and constant. This gives the desired equality.

3. Note that $\wp'(z)$ is odd, it has zeroes of order 2. Indeed, if $z \equiv -z \pmod{\Lambda}$ then $\wp'(z) = \wp'(-z) = -\wp'(z) \Rightarrow \wp'(z) = 0$. Letting $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, the order two points are $\omega_i/2, i = 1, 2$ and $\omega_3/2 = (\omega_1+\omega_2)/2$. Clearly, $\wp'(\omega_i/2) = 0, i = 1, 2, 3$. From the previous part, $\wp(\omega_i/2)$ are roots of the polynomial $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ and hence the said factorisation works.

□

Remark 6.2.10.

- $\wp(z)$ is an even function.
- The roots $e_i's$ in the previous proposition are distinct. Note that $\wp(z) - e_1$ vanishes at $z = \omega_1/2$. This is a double zero since $\wp'(\omega_1/2) = 0$. Similarly, $\wp(z) - e_2$ has double zero at $z = \omega_2/2$. If $e_1 = e_2$ then $\wp(z) - e_1$ would have zero of order 4 a contradiction. Therefore $e_1 \neq e_2$. Similarly, $e_1 \neq e_3, e_2 \neq e_3$.

6.2.3. Isogenies

Definition 6.2.11.
A non-zero holomorphic homomorphism between complex tori is called an isogeny.

6.3. Enhanced elliptic curves

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

Definition 6.3.1.

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

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

Proof. □

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

7.1. Riemann surfaces

Proposition 7.1.1.
The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ is properly discontinuous, i.e., for $z_1, z_2 \in \mathcal{H}$ 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. □

Corollary 7.1.2.
$Y(\Gamma) = \Gamma\backslash\mathcal{H}$ with the quotient topology is Hausdorff.

Proof. □

Proposition 7.1.3.
$X(\Gamma)$ is compact.

Proof. □

Definition 7.1.4.
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 7.1.5.
A point $P \in Y(\Gamma)$ is called an elliptic point if for any lift z of P in $\mathcal{H}$, 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.

Theorem 7.1.6.
$Y(\Gamma)$ is a Riemann surface.

Proof. □

Theorem 7.1.7.
$X(\Gamma)$ is a Riemann surface.

Proof. □

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): More Riemann surfaces

8.1. Riemann surfaces contd..

9. Lecture-9 (7th February, 2023): Riemann surfaces and Riemann Roch theorem

Corollary 9.0.1.
Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then,

$$g(X(\Gamma)) = 1 + \frac{N}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{4} - \frac{\epsilon_\infty}{2}$$

where $N = [\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma}]$, ϵ_2 is the number of elliptic points of order 2, ϵ_3 is the number of elliptic points of order 3 and ϵ_∞ is the number of cusps of $\Gamma = \#(\Gamma \backslash \mathbb{P}^1(\mathbb{Q}))$.

Proof. Consider the map

$$X(\Gamma) \xrightarrow{f} X(\mathrm{SL}_2(\mathbb{Z}))$$

with $\deg f = n$. Then,

$$2g(X(\Gamma)) - 2 = N(-2) + \sum_{Q \in X(\Gamma)} (e_Q - 1)$$

If $f(Q)$ is not equivalent to i or ω, Q is unramified.

If $f(Q)$ is equivalent to i, then we have two cases:

1. Q is elliptic implies Q is unramified.
2. Q is not elliptic implies $e_Q = 2$.

$$\sum_{Q \in f^{-1}([i])} e_Q = N, \sum_{Q \in f^{-1}([i])} (e_Q - 1) = \frac{N - \epsilon_2}{2}$$

If $f(Q) \sim \omega$, then

$$\sum_{Q \in f^{-1}([i])} (e_Q - 1) = \frac{2(N - \epsilon_3)}{3}$$

Finally, let us talk about ramification at the cusps. Recall from the charts at cusps that Local coordinate at a cusp Q is $e^{2\pi i/h}$ for some integer $h \geq 1$. In this case $e_Q = h$ and

$$\sum_{Q \in f^{-1}([i])} (e_Q - 1) = \left(\sum_Q e_Q \right) - \epsilon_\infty = N - \epsilon_\infty$$

Therefore,

$$2g(X(\Gamma)) = -2N + \frac{N-\epsilon_2}{2} + 2\frac{N-\epsilon_3}{3} + N - \epsilon_\infty$$
$$2g(X(\Gamma)) = \frac{N}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{6} - \frac{\epsilon_\infty}{2} + 1$$

□

Exercise 9.0.2. $g(X(\Gamma_0(p))) = 0$ *iff* $p \in \{2, 3, 5, 6, 7, 13\}$

Goal of the day

$$\dim_{\mathbb{C}} M_k(\Gamma) = (k-1)(g(X(\Gamma)) - 1) + \frac{k}{2}\epsilon_\infty + \left[\frac{k}{4}\right]\epsilon_2 + \left[\frac{k}{3}\right]\epsilon_3$$

and

$$\dim_{\mathbb{C}} S_k(\Gamma) = (k-1)(g(X(\Gamma)) - 1) - \frac{k}{2}\epsilon_\infty + \left[\frac{k}{4}\right]\epsilon_2 + \left[\frac{k}{3}\right]\epsilon_3$$

To proceed we will need some algebraic geometry language.

$$\begin{aligned} X - &\text{ is a smooth projective curve over } \mathbb{C} \\ \mathcal{O}_X - &\text{ structure sheaf} \\ \mathcal{O}_X(U) - &\{f : U \to \mathbb{C} \text{ regular for open } U\} \\ \mathcal{F}(U) - &\mathcal{O}_X\text{- module sheaves} \end{aligned}$$

We are concerned with invertible $\mathcal{O}_X$-module sheaves, i.e., locally free of rank 1. These are called invertible sheaves.

Example 9.0.3.
For a number field F, take $\mathcal{O}_F$ as the structure sheaf. Any nonzero fractional ideal is invertible hence we can think of that as the invertible sheaves.

Invertible sheaves form a group under $\otimes_{\mathcal{O}_X}$.

$H^0(X, \mathcal{F}) =$ global sections.

Remark 9.0.4.
As X is a smooth projective curve, $H^0(X, \mathcal{F}) = \mathbb{C}$. This is like Liouville's theorem.

We can take a look at meromorphic sections of $\mathcal{F}$

$$\mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathrm{Frac}(\mathcal{O}_X(U))$$

where $\mathrm{Frac}(\mathcal{O}_X(U))$ are the meromorphic functions.

Theorem 9.0.5 (Riemann existence theorem)**.**
An invertible sheaf on a compact Riemann surface has a non-constant global meromorphic section.

Definition 9.0.6.
Let $\mathcal{F}$ be an invertible sheaf on X. Take a non-constant global section s of $\mathcal{F}$. We define $\deg(\mathcal{F})$ to be the sum of orders of zeros of s.

Remark 9.0.7.
Note that this definition does not depend on the choice of s. If we take a different s', then $s = fs'$ where f is a global meromorphic section of $\mathcal{O}_X$ ($\deg f = 0 =$ sum of orders of zeros)

Proposition 9.0.8.
Properties of the degree function:

1. $\deg(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}) = \deg \mathcal{F} + \deg \mathcal{G}$
2. $\deg \mathcal{F}^{-1} = -\deg \mathcal{F}$

Theorem 9.0.9 (Riemann-Roch theorem)**.**
1. $H^0(X, \mathcal{F})$ is a finite dimensional $\mathbb{C}$-vector space.
2. Put $h^0(X, \mathcal{F}) = \dim_{\mathbb{C}} H^0(X, \mathcal{F})$. Then,
$$h^0(X, \mathcal{F}) - h^0(X, \Omega^1_X \otimes \mathcal{F}^{-1}) = 1 - g(X) + \deg \mathcal{F}$$
where $\Omega = \Omega^1_X$ is the sheaf of holomorphic differentials on X.

Remark 9.0.10 (Facts)**.**
1. If $\deg \mathcal{F} < 0$, then $H^0(X, \mathcal{F}) = 0$
2. If $\deg \mathcal{F} >> 0$, then $H^0(X, \Omega \otimes \mathcal{F}^{-1}) = 0$

Lemma 9.0.11.
1. $h^0(X, \Omega) = g(X)$
2. $\deg \Omega = 2g - 2$

Proof.
1. Take $\mathcal{F} = \mathcal{O}_X$. Then
$$\begin{aligned} h^0(X, \mathcal{O}_X) - h^0(X, \Omega \otimes_{\mathcal{O}_X} \mathcal{O}_X^{-1}) &= 1 - g(X) + \deg \mathcal{O}_X \\ 1 - h^0(X, \Omega) &= 1 - g(X) + 0 \\ g(X) &= h^0(X, \Omega) \end{aligned}$$

2. Take $\mathcal{F} = \Omega$. Then,

$$h^0(X, \Omega) - h^0(X, \Omega_X) = 1 - g(X) + \deg \Omega$$
$$g(X) - 1 = 1 - g + \deg \Omega$$

□

Lemma 9.0.12.

Definition 9.0.13 (Katz sheaf)**.**
Let $X(\Gamma), k \in \mathbb{Z}$ be as usual. For V open in $X(\Gamma)$, we define a sheaf ω_k as

$$\omega_k = \{f : \pi^{-1}(V) \subseteq \mathcal{H} \to \mathbb{C}\}$$

with f is holomorphic and $f(\gamma \cdot z) = (cz + d)^k f(z)\ \forall\ \gamma \in \Gamma, \forall\ z \in \pi^{-1}(V)$ and $\pi : \mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) \to X(\Gamma)$

Remark 9.0.14.
$H^0(X(\Gamma), \omega_k)$ gives modular forms of weight k and level Γ.

Theorem 9.0.15. 1. ω_k is an invertible sheaf.

2. $\omega_2 = \Omega$ (cusps).

Let $\mathcal{L}$ be an invertible sheaf, $D = \sum_i n_i P_i$ divisor of X (P_i is a point of X). If x is a meromorphic section of $\mathcal{L}$, then

$$\operatorname{div}(x) := \sum_{P \in X} \operatorname{ord}_P(x)$$

and

$$\mathcal{L}(D) = \{x,\ \text{a meromorphic section of } \mathcal{L} : \operatorname{div}(x) + D \geq 0\}$$

Example 9.0.16.
If P is a point of X. Then,

$$\mathcal{L}(-P) = \text{ meromorphic section } x \text{ of } \mathcal{L} \text{ with atleast a simple zero of } P$$
$$\mathcal{L}(P) = \text{meromorphic section } x \text{ of } \mathcal{L} \text{ with atmost a simple pole at } P$$

Definition 9.0.17.

$$\text{cusps} = \sum_{P \in \Gamma \backslash \mathbb{P}^1(\mathbb{Q})} P$$

If Γ is a congruence subgroup. Then,

$$\Gamma_\infty = \{g \in \Gamma : g \cdot \infty = \infty\}$$

has one of the following forms $\{\pm I_2\}, \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle - \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle$

Definition 9.0.18.

1. ∞ is called irregular cusp for Γ if $\Gamma_\infty = \left\langle - \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle$
2. A cusp s is called irregular if ∞ is irregular for $\alpha\Gamma\alpha^{-1}$ where $s = \alpha \cdot \infty (\alpha \in \mathrm{SL}_2(\mathbb{Z}))$

Definition 9.0.19.
Let r be the least common multiple of integers in the following set

$$\{\mathrm{Stab}_\Gamma(P), P \in \mathbb{H}\} \cup \{2 \text{ if there exists an irregular cusp}\}$$

Exercise 9.0.20. $1 \leq r \leq 12$

Definition 9.0.21.
Γ is called neat if $r = 1$.

Exercise 9.0.22.

1. *$\Gamma_0(N)$ is neat for $N \geq 5$.*
2. *If Γ is neat, then it has no elliptic points and $-I \notin \Gamma$*

Theorem 9.0.23.
If Γ is neat, then for any $k \geq 0$, we have

$$\dim_{\mathbb{C}} M_k(\Gamma) = (k-1)(g(X(\Gamma)) - 1) + \frac{k}{2}\epsilon_\infty$$

and

$$\dim_{\mathbb{C}} S_k(\Gamma) = (k-1)(g-1) + \left[\frac{k}{4}\right]\epsilon_2 + \left[\frac{k}{3}\right]\epsilon_3 + \frac{k-1}{2}\epsilon_\infty$$

Remark 9.0.24 (Fact)**.**
For an integer r as above, we have $\omega_{k+r} = \omega_k \otimes \omega_r$

In particular, if $r = 1$, then $\omega_r = \omega_1^{\otimes r} = \omega^{\otimes r}$

Proof of theorem.

$$\begin{aligned}\deg \omega &= \frac{1}{2} \deg \omega^{\otimes 2} \\ &= \frac{1}{2} \deg(\Omega(\text{cusps})) \\ &= \frac{1}{2}(\deg \Omega + \epsilon_\infty) \\ &= g - 1 + \frac{\epsilon_\infty}{2}\end{aligned}$$

$\therefore$

$$\begin{aligned}h^0(X(\Gamma), \omega_k) - h^0(X, \Omega \otimes (\omega^{\otimes k})^{-1}) &= \deg(\omega^{\otimes(-k)}) - g + 1 \\ &= (k-1)(g-1) + \frac{k}{2}\epsilon_\infty\end{aligned}$$

□

10. Lecture-10 (9th February, 2023): Automorphic forms, j-invariant and Riemann-Roch

10.1. Automorphic forms

Let $\widehat{\mathbb{C}}$ be the compactified Riemann sphere $\mathbb{C} \cup \{\infty\}$.

Let $V \subseteq \mathbb{C}$ be open. $f : V \to \widehat{\mathbb{C}}$ is meromorphic if either $f \equiv 0$ or f has a Laurent series expansion

$$f(z) = \sum_{n=m}^{\infty} a_n (z-\tau)^n \text{ for every } \tau \in V, a_m \neq 0 \tag{10.1}$$

The order of vanishing of f at τ is $v_\tau(f) = m$.

Recall that f is weakly modular if $f : \mathbb{H} \to \widehat{\mathbb{C}}$ is meromorphic and $f(\gamma \cdot z) = (cz+d)^k f(z)\ \forall\ \gamma \in \Gamma$

f has a q-expansion at ∞, namely

$$f(z) = \sum_{-\infty}^{\infty} a_n q_h^n \text{ where } q_h = \exp(w\pi z/h) \tag{10.2}$$

f is meromorphic at ∞ if $f(z) = \sum_{n=m}^{\infty} a_n q_h^n$ with $a_m \neq 0$ and $v_\infty(f) = m$

Definition 10.1.1.
$\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and $k \in \mathbb{Z}$. A function $f : \mathbb{H} \to \widehat{\mathbb{C}}$ is an automorphic form of weight k wrt Γ if

1. f is meromorphic
2. $f(\gamma z) = (cz+d)^k f(z)\ \forall\ \gamma \in \Gamma, \forall\ z \in \mathbb{H}$
3. $f|_{k,\gamma}$ is meromorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$

We denote the space of automorphic forms of weight k and level Γ by $\mathcal{A}_k(\Gamma)$

Example 10.1.2.

$$j(z) = 1728\frac{g_2^3}{\Delta(z)} \tag{10.3}$$

Recall that $g_2(z)$ is the Eisenstein series of weight 4 and level $\mathrm{SL}_2(\mathbb{Z})$ and $\Delta(z)$ is the cusp form of weight 12 and level $\mathrm{SL}_2(\mathbb{Z})$.

$\mathcal{A}_0(\Gamma)$ is the field of automorphic forms on $X(\Gamma)$. We have already seen that $X(\mathrm{SL}_2(\mathbb{Z})) \cong \mathbb{P}^1(\mathbb{C})$ and the function field of $\mathbb{P}^1(\mathbb{C}) \cong \mathbb{C}(X)$

Proposition 10.1.3.
$\mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}(j)$

Proof. Suppose $j \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z})), \mathbb{C}(j) \subseteq \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$.
Let $g \in \mathcal{A}_0(\mathrm{SL}_2(\mathbb{Z}))$ and $z_1, \ldots, z_r$ be zeroes of g and $p_1, \ldots, p_s$ be the poles of g (with multiplicities). Then define

$$f(z) = \frac{\prod_{i=1}^{r}(j(z) - j(z_1))}{\prod_{i=1}^{s}(j(z) - j(p_i))} \in \mathbb{C}(j)$$

Clearly, f has the same number of zeroes as g on $\mathbb{H}$. Hence, f, g also have zeros of same order at ∞ (for a meromorphic function on $X(\mathrm{SL}_2(\mathbb{Z}))$ the sum of zeros at all points is 0). This implies that $g = cf \in \mathbb{C}(j)$. □

Remark 10.1.4 (Fact)**.**
$\mathcal{A}_0(\Gamma_0(N)) = \mathbb{C}(j, j_N)$ where $j_N(z) = j(Nz)$

We define the order of vanishing of function on $X(\Gamma)$ as follows:

Let $\tau \in \mathbb{H}$ and

$$\begin{array}{ccc} \pi : \mathbb{H}^* & \longrightarrow & X(\Gamma) \\ & \overset{g}{\searrow} & \downarrow f \\ & & \mathbb{C} \end{array}$$

Then,

$$v_\pi(\tau)(g) \quad = \frac{v_\tau(f)}{h} \in \mathbb{Q} \tag{10.4}$$

where h is the order of stabiliser of τ and this equals $\#(\{\pm I_2\Gamma_\tau/\{\pm I_2\}\})$

If τ is a cusp, $\Gamma_\infty = \{I_2\}\langle$ and thus we define

$$v_{\pi(\infty)}(f) = \begin{cases} v_\infty(f)/2 & \Gamma_\infty = \langle - \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \\ v_\infty(f) & \text{otherwise} \end{cases}$$

10.2. Riemann-Roch theorem

Back to Riemann-Roch again.

Let X be a compact Riemann surface. A divisor on X is a finite linear combination $\sum_{x\in X(\Gamma)} n_x x, n_x \in \mathbb{Z}$ and $n_x = 0$ for almost all x. The divisors $\mathrm{Div}(X)$ forms a free abelian group on X.

$$\deg : \mathrm{Div}(X) \longrightarrow \mathbb{Z} \tag{10.5}$$
$$\sum n_x x \mapsto \sum n_x \tag{10.6}$$

The kernel of this map is denoted by $\mathrm{Div}^0(X)$

Next,

$$\mathrm{div} : \mathbb{C}(X)^\times \longrightarrow \mathrm{Div}(X) \tag{10.7}$$
$$f \mapsto \textstyle\sum_x v_x(f)x \tag{10.8}$$

Exercise 10.2.1. *In fact,* $\deg(\mathrm{div}(f)) = 0$

Let $D \in \mathrm{Div}(X)$. We define

$$L(D) = \{f \in \mathbb{C}(X) : f = 0 \text{ or } \mathrm{div}(f) + D \geq 0\} \tag{10.9}$$

Define $\ell(D) = \dim_{\mathbb{C}} L(D)$.

Remark 10.2.2.
A fact to be noted is that $\ell(D) < \infty$.

Theorem 10.2.3 (Riemann-Roch theorem)**.**
X is a compact Riemann surface of genus g. Let λ be an $\mathcal{O}_X$ module generator of Ω^1_X ($\mathrm{div}(\lambda)$ is called the canonical divisor). Then, for any $D \in \mathrm{Div}^0(X)$ we have

$$\ell(D) - \ell(\mathrm{div}(\lambda) - D) = \deg D - g + 1 \tag{10.10}$$

Theorem 10.2.4.
Let k be an even integer. Then,

$$\dim_{\mathbb{C}} M_k(\Gamma) = \begin{cases} (k-1)(g-1) + \left[\frac{k}{4}\right]\epsilon_2 + \left[\frac{k}{3}\right]\epsilon_3 + \frac{k-1}{2}\epsilon_\infty & k \geq 2 \\ 1 & k = 0 \\ 0 & k < 0 \end{cases} \tag{10.11}$$

$$\dim_{\mathbb{C}} S_k(\Gamma) = \begin{cases} \dim_{\mathbb{C}} M_k(\Gamma) - \epsilon_\infty & k \geq 4 \\ g & k = 2 \\ 0 & k \leq 0 \end{cases} \tag{10.12}$$

Proof. Note that $\mathrm{Div}_{\mathbb{Q}}(X(\Gamma))$ is a $\mathbb{Q}$ vector space generated by points of $X(\Gamma)$.

For $\sum n_x x \in \mathrm{Div}_{\mathbb{Q}}(X(\Gamma))$ put

$$\left[\sum n_x x\right] = \sum [n_x] x \tag{10.13}$$

Take $\omega \in \Omega^{\otimes k/2}(X(\Gamma))$ and $D = \mathrm{div}(\omega)$ □

Theorem 10.2.5.
Let k be an odd integer. If $-I_2 \in \Gamma$, then $M_k(\Gamma) = S_k(\Gamma) = 0$.

Assume $-I_2 \notin \Gamma$, then

$$\dim_{\mathbb{C}} M_k(\Gamma) = \begin{cases} (k-1)(g-1) + \left[\frac{k}{3}\right] \epsilon_3 + \frac{k}{2}\epsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\epsilon_\infty^{\mathrm{irr}} & k \geq 3 \\ 0 & k < 0 \end{cases} \tag{10.14}$$

and

$$\dim_{\mathbb{C}} S_k(\Gamma) = \begin{cases} \dim_{\mathbb{C}} M_k(\mathbb{C}) - \epsilon_\infty^{\mathrm{reg}} & k \geq 3 \\ 0 & k < 2 \end{cases} \tag{10.15}$$

This leaves us with the case $k = 1$.

11. Lecture-11 (14th February, 2023): Cusps of Congruence subgroups

Goal: We want to find the number of cusps of level Γ for various congruence subgroups Γ.

Recall that cusps of level Γ is the set $\gamma\backslash\mathbb{P}(\mathbb{Q})$. We work with $\mathbb{Q}\times\mathbb{Q}$ instead of $\mathbb{P}^1(\mathbb{Q})$

Lemma 11.0.1.
If $s=a/c, s'=a'/c'$ are two elements of $\mathbb{Q}\cup\{\infty\}$. Then,

$$\begin{pmatrix}a'\\c'\end{pmatrix}=\pm\gamma\begin{pmatrix}a\\c\end{pmatrix}\Leftrightarrow s'=\gamma\cdot s$$

Here, the rationals are taken in reduced form.

Remark 11.0.2.
Action of $\mathrm{SL}_2(\mathbb{Z})/\{\pm\mathbf{Id}_2\}$ on $\mathbb{P}^1(\mathbb{Q})$ corresponds to left multiplication by elements of $\mathrm{SL}_2(\mathbb{Z})$ on columns $\begin{pmatrix}a\\c\end{pmatrix}\in\mathbb{Z}^2$ such that $\gcd(a,c)=1$

Proposition 11.0.3.
Let $s=a/c, s'=a'/c'\in\mathbb{P}^1(\mathbb{Q})$. Then,

1. $\Gamma(N)\cdot s=\Gamma\cdot s'\Leftrightarrow\pm\begin{pmatrix}a\\c\end{pmatrix}\equiv\begin{pmatrix}a'\\c'\end{pmatrix}\pmod N$
2. $\Gamma_1(N)\cdot s=\Gamma_1\cdot s'\Leftrightarrow\begin{pmatrix}a+jc\\c\end{pmatrix}\equiv\begin{pmatrix}a'\\c'\end{pmatrix}\pmod N$ for some j
3. $\Gamma_0(N)\cdot s=\Gamma_0\cdot s'\Leftrightarrow\pm\begin{pmatrix}a+jc\\yc\end{pmatrix}\equiv\begin{pmatrix}ya'\\c'\end{pmatrix}\pmod N$

Lemma 11.0.4.
Let $a,c\in\mathbb{Z}$ and $\bar a,\bar c$ be their images in $\mathbb{Z}/N\mathbb{Z}$. TFAE:

1. $\begin{pmatrix}\bar a\\\bar c\end{pmatrix}\in(\mathbb{Z}/N\mathbb{Z})^2$ has a lift $\begin{pmatrix}a'\\c'\end{pmatrix}\in\mathbb{Z}^2$ with $\gcd(a',c')=1$
2. $\gcd(a,c,N)=1$

3. $\begin{pmatrix} \bar{a} \\ \bar{c} \end{pmatrix}$ has order N in $(\mathbb{Z}/N\mathbb{Z})^2$.

Proof. $1 \Leftrightarrow 2$ has been done earlier.
Now let us show $3 \Leftrightarrow 2$.
Suppose $k \begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{N}$. Then, $ka \equiv 0 \equiv kc \pmod{N} \Rightarrow k \gcd(a, c) \equiv 0 \pmod{N}$. We know that $N \mid k$ and this can happen iff no non-trivial factors of N divides $\gcd(a, c)$ or equivalently $\gcd(a, c, N) = 1$. □

Proposition 11.0.5.

$$\#\mathrm{Cusps}(\Gamma(N)) = \begin{cases} \frac{1}{2} \sum_{d|N} \frac{N}{d} \varphi(d)\varphi(N/d) \\ = \frac{1}{2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right) & \text{if } N > 2 \\ 3 & \text{if } N = 2 \end{cases}$$

Proof. □

12. Lecture-12 (16th February, 2023): More about cusps

Part II.

Elliptic Curves

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

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

14.1. Affine Varieties

Suppose k is a perfect field (every extension is separable) like Q any field of characteristic 0 or any finite field.
Let $G_{\bar{k}/k}$ be the Galois group of the extension $\bar{k}/k$ where $\bar{k}$ is the algebraic closure of k.

Definition 14.1.1.
An afffine n-space over k denoted by $\mathbb{A}^n(\bar{k})$ or $\mathbb{A}^n$ is the set

$$\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \{P = (x_1, \ldots, x_n) : x_i \in \bar{k}\} \tag{14.1}$$

The set of k-rational points of $\mathbb{A}^n$ is the set

$$\mathbb{A}^n = \mathbb{A}^n(k) = \{P = (x_1, \ldots, x_n) : x_i \in k\} \tag{14.2}$$

The Galois group $G_{\bar{k}/k}$ acts on $\mathbb{A}^n$ as follows: Take $\sigma \in \mathrm{Gal}(\bar{k}/k)$ then

$$\sigma P = (\sigma x_1, \ldots, \sigma x_n) \tag{14.3}$$

Therefore, k-rational points can also be realised as

$$\mathbb{A}^n(k) = \{P \in \mathbb{A}^n : \sigma P = P \; \forall \; \sigma \in G_{\bar{k}/k}\} \tag{14.4}$$

Definition 14.1.2.
Let $\bar{k}[X_1, \ldots, X_n]$ be the polynomial ring and I be an ideal in the ring. Then, we associate a set I to this ideal as follows:

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \; \forall \; f \in I\} \tag{14.5}$$

An affine algebraic set is a set of the form V_I for some ideal I.

Theorem 14.1.3 (Hilbert Basis theorem)**.**
All ideals of $k[\mathbf{X}]$ is finitely generated.

Definition 14.1.4.
If V is an algebraic set, then we associate an ideal $I(V)$ as

$$I(V) = \{f \in \bar{k}[\mathbf{X}] : f(P) = 0 \ \forall \ P \in V\} \tag{14.6}$$

An algebraic set is said to be defined over k if its ideal $I(V)$ is generated by polynomials in $k[\mathbf{X}]$ and we denote this by V/k. If V is defined over k, then the set of k-rational points is just

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

Remark 14.1.5.
Let V be an algebraic set and consider the ideal $I(V/k)$ defined by

$$I(V/k) = \{f \in k[\mathbf{X}] : f(P) = 0 \ \forall \ P \in V\} = I(V) \cap k[\mathbf{X}] \tag{14.7}$$

Then we see that V is defined over k iff

$$I(V) = I(V/k)\bar{k}[\mathbf{X}]$$

If V is defined over k and $f_1, \ldots, f_r \in k[\mathbf{X}]$ be the generators of $I(V/k)$. Then, $V(k)$ is precisely the set of solutions $P = (x_1, \ldots, x_n)$ to the simultaneous polynomial equations

$$f_1(P) = \cdots = f_r(P) = 0 \text{ where } x_i \in k \tag{14.8}$$

Note that if $f(\mathbf{X}) \in k[\mathbf{X}], P = (x_1, \ldots, x_n)$ and $\sigma \in G_{\bar{k}/k}$, then

$$f(\sigma P) = a_0 + a_1\sigma P + \cdots + a_m(\sigma P)^m = \sigma f(P) \tag{14.9}$$

Hence, if V is defined over k, then the action of $G_{\bar{k}/k}$ on $\mathbb{A}^n$ induces an action on V and clearly,

$$V(k) = \{P \in V : \sigma P = P \ \forall \ \sigma \in G_{\bar{k}/k}\} \tag{14.10}$$

Example 14.1.6.
Let $V = \{(x, y) \in \mathbb{A}^2 : x^2 - y^2 = 1\}$. Then, $I(V) = \langle X^2 - Y^2 - 1\rangle$ and therefore V is defined over k.

Example 14.1.7.
The algebraic set $V : X^n + Y^n = 1$ is defined over $\mathbb{Q}$.

Example 14.1.8.
The algebraic set $V : Y^2 = X^3 + 17$ has many $\mathbb{Q}$-rational points (infact infinitely many).

Definition 14.1.9.
An affine algebraic set V is called an affine variety if $I(V)$ is prime ideal in $\bar{k}$.

Remark 14.1.10.
It is not enough to check that $I(V/k)$ is prime in $k[\mathbf{X}]$ to conclude whether $I(V)$ is prime in $\bar{k}[\mathbf{X}]$. For example, consider the ideal $\langle X^2 - 2Y^2 \rangle$ in $\mathbb{Q}[X, Y]$

Definition 14.1.11.
Let V/k be a variety defined over k. Then the affine coordinate ring of V/k is defined by

$$k[V] = \frac{k[\mathbf{X}]}{I(V/k)} \tag{14.11}$$

The ring $k[V]$ is an integral domain. Its quotient field is denoted by $k(V)$ and is called the function field of V/k. Similarly, $\bar{k}(V)$ and $k(V)$ are defined by replacing k by $\bar{k}$.

Definition 14.1.12.
Let V be a variety. The dimension of V, denoted by $\dim(V)$ is the transcendence degree of $\bar{k}(V)$ over $\bar{k}$.

Example 14.1.13.
The dimension of $\mathbb{A}^n$ is n since $\bar{k}(\mathbb{A}^n) = \bar{k}(X_1, \ldots, X_n)$. Similarly, if $V \subseteq \mathbb{A}^n$ is given by a single polynomial f, then the dimension of V is $n - 1$,

Definition 14.1.14.
Let V be a variety, $P \in V$ and $f_1, \ldots, f_m \in \bar{k}[\mathbf{X}]$ a set of generators for $I(V)$. Then, V is nonsingular (or smooth) at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j} \right)_{1 \leq i \leq m 1 \leq j \leq n}$$

has rank $n - \dim V$. If V is non-singular at every point, then we say that V is non-singular or smooth.

Example 14.1.15.
Let V be a variety corresponding to a single nonconstant polynomial f. Then,

$\dim V = n - 1$ and $P \in V$ is regular iff

$$\frac{\partial f}{\partial X_1}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0 \tag{14.12}$$

Example 14.1.16.
Consider the two varieties $V_1 : Y^2 = X^3 + X, V_2 : Y^2 = X^3 + X^2$. Then, from previous example the singular points on V_1, V_2 are given by $V_1^{\text{sing}} : 3X^2 + 1 = 2Y = 0$ and $V_2^{\text{sing}} : 3X^2 + 2X = 2Y = 0$. Clearly, V_1 is non-singular and V_2 has one singular point $(0, 0)$.

We also have another way to determine smoothness using the functions on the variety V.

Definition 14.1.17.
For each $P \in V$, we define an ideal M_P of $\bar{k}[V]$ by

$$M_P = \{f \in \bar{k}[V] : f(P) = 0\}$$

This ideal is a maximal ideal as it is the kernel of the map

$$\begin{aligned} \bar{k}[V] &\to \bar{k} \\ f &\mapsto f(P) \end{aligned}$$

The quotient M_P/M_P^2 is a finite dimensional $\bar{k}$-vector space.

Proposition 14.1.18.
Let V be a variety. A point $P \in V$ is non-singular iff $\dim_{\bar{k}} M_P/M_P^2 = \dim V$.

Example 14.1.19.
Consider the point $P = (0, 0)$ and the two varieties V_1, V_2 as in previous example. Then in both the cases M_P is generated by X, Y which implies M_P^2 is ideal generated by X^2, XY, Y^2.

For V_1, $X = Y^2 - X^3 \equiv 0 \pmod{M_P^2}$ and thus M_P/M_P^2 is generated by Y alone.

For V_2, there is no nontrivial relationship between X, Y modulo M_P^2 therefore M_P/M_P^2 requires both X, Y as generators. Since $\dim V_i = 1$ therefore V_1 is smooth but V_2 is not.

Proposition 14.1.20.
The local ring of V at P, denoted by $\bar{k}[V]_P$ is the localisation of $\bar{k}[V]$ at M_P.

$$\bar{k}[V]_P = \{F \in \bar{k}(V) : F = f/g \text{ for some } f, g \in \bar{k}[V], g(P) \neq 0\} \tag{14.13}$$

The functions in $\bar{k}[V]_P$ are called regular functions at P.

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

15.1. Projective varieties

Definition 15.1.1.
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 15.1.2.
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 15.1.3.
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 15.1.4.
An ideal $I \subseteq \bar{k}[X_0, \ldots, X_n]$ is called a homogenous ideal if it is generated by homogenous polynomial.

Definition 15.1.5.
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 15.1.6.

- 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 $\{f \in \bar{k}[X_0 \ldots, X_n] \mid f$ 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 15.1.7.
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 15.1.8.
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 15.1.9.
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 15.1.10.
$V \subseteq \mathbb{P}^2$ 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 15.1.11.
$V : 3X^3 + 4Y^3 + 5Z^3 = 0$. $V(\mathbb{Q}) = \emptyset$ but for all prime p we have $V(\mathbb{Q}_p) \neq \emptyset$

Definition 15.1.12.
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 15.1.13.
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 15.1.14.
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 15.1.15.
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 15.1.16.
$V : Y^2 = X^3 + 17 \subseteq \mathbb{A}^2 \to \mathbb{P}^2$ with $(X, Y) \mapsto [X : Y : 1]$. Here, $\overline{V} : Y^2Z = X^3 + 17Z^3$ and $\overline{V} \backslash V = \{[0 : 1 : 0]\}$

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

16.1. Projective varieties contd..

Definition 16.1.1.

- 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 16.1.2.
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 16.1.3.
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 $(X_0, \ldots, X_n)$

16.2. Maps between varieties

Definition 16.2.1.
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 16.2.2.
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 16.2.3.
ϕ is defined over k iff $\phi = \sigma(\phi)\ \forall\ \sigma \in G(\bar{k}/k)$.

Definition 16.2.4.
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 16.2.5.
A rational map is called a morphism if it is regular everywhere.

Remark 16.2.6.
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 16.2.7.
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 16.2.8.
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 16.2.9.
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 16.2.10.
$\mathrm{char}(k) \neq 2$, $V : X^2 + Y^2 = Z^2$.

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

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 16.2.11.

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

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

Example 16.2.12.
$V : Y^2Z = X^3 + X^2Z$

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

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 16.2.13.
$V_1 : X^2+Y^2 = Z^2, V_2 : X^2+Y^2 = 3Z^2$. $V_1 \ncong V_2$ over $\mathbb{Q}$ but $V_1 \cong V_2$ over $\mathbb{Q}(\sqrt{3})$.

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

17.1. Curves

Definition 17.1.1.
A curve is a projective variety of dimension 1.

Example 17.1.2.
Vanishing set of an irreducible polynomial in $\mathbb{P}^2$.

Proposition 17.1.3.
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 17.1.4.
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 17.1.5.
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 17.1.6.
If C is defined over k, we can find a unit $t \in k(C)$.

Definition 17.1.7.
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 17.1.8.
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 17.1.9.
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 17.1.10.
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.

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

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

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

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. □

17.2. Morphism between curves

Proposition 17.2.1.
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 17.2.2.
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 17.2.3. 1. $V : X^2 + Y^2 = Z^2$

18. Lecture-6 (19th January, 2023): Morphisms between curves, ramification and Frobenius map

18.1. Morphisms between curves contd..

Theorem 18.1.1.
If $\phi : C_1 \to C_2$ are morphisms of curves, then ϕ is either surjective or constant.

Let $C_1, C_2/k$ be two curves over k and $\phi : C_1, C_2$ nonconstant rational map defined over k. Then, we obtain a map

$$\phi^* : k(C_2) \to k(C_1) \text{ such that } f \mapsto f \circ \phi$$

Theorem 18.1.2.
Let C_1, C_2 be two curves defined over k.

1. Suppose $\phi : C_1 \to C_2$ be two nonconstant rational maps defined over k. Then $k(C_1)$ is a finite extension of $\phi^*(k(C_2))$.
2. Suppose $i : k(C_2) \to k(C_1)$ is an injection of function fields. Then there exists an unique rational map $\phi : C_1 \to C_2$ defined over k such that $\phi^* = i$.
3. Suppose $\mathbb{K} \subseteq k(C_1)$ be a subfield containing k and of finite index. Then there exists a smooth curve C'/k unique upto isomorphism and a non-constant rational map $\phi : C_1 \to C'$ defined over k such that $\phi^*(k(C_1)) = \mathbb{K}$

Definition 18.1.3.
Let $\phi : C_1 \to C_2$ be a morphism of curves defined over k. If ϕ is constant, then $\deg \phi := 0$. Otherwise,

$$\deg \phi = [k(C_1) : \phi^*(k(C_2))]$$

- ϕ is separable if $k(C_1)/\phi^*(k(C_2))$ is separable.
- ϕ is inseparable if $k(C_1)/\phi^*(k(C_2))$ is inseparable.
- ϕ is purely inseparable if $k(C_1)/\phi^*(k(C_2))$ is purely inseparable.

Denote the separable and inseparable degree of $k(C_1)/\phi^*(k(C_2))$ by $\deg_s \phi$ and $\deg_i \phi$ respectively.

Definition 18.1.4.
Let $\phi : C_1 \to C_2$ be a morphism of curves defined over k. Then $k(C_1)$ is a finite extension of $\phi^*(k(C_2))$, We wish this to construct a map

$$\phi_* : k(C_1) \to k(C_2) \qquad \phi_* = \phi^* \circ \mathrm{Nm}_{k(C_1)/\phi^*(k(C_2))} \tag{18.1}$$

Proposition 18.1.5.
Let $f(X) \in k[X]$ be of degree 4 with $\mathrm{disc}(f) \neq 0$. Then there is a smooth projective curve in $\mathbb{P}^3$ satisfying

1. $C \cap \mathbb{A}^3 \cong$ affine curve $Y^2 = f(X)$
2. $f(X) = a_0X^4 + \cdots + a_4$. Then $C \cap \{X_0 = 0\}$ consists of two points $[0, 0, \pm\sqrt{a_0}, 1]$

18.2. Ramification

Definition 18.2.1.
Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves and $P \in C_1$. Ramification index of ϕ at P is defined by

$$e_\phi(P) := \mathrm{ord}_P(\phi^*(t_{\phi(P)}))$$

where $t_{\phi(P)} \in k(C_2)$ is a uniformizer at $\phi(P)$.

- ϕ is unramified at P if $e_\phi(P) = 1$
- If ϕ is unramified at all points of C_1, then we say ϕ is unramified.

Proposition 18.2.2.
Let $\phi : C_1 \to C_2$ be a non-constant morphism of smooth curves.

1. For all $Q \in C_2$
$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi \tag{18.2}$$
2. For all but finitely many $Q \in C_2$
$$\#\phi^{-1}(Q) = \deg_s \phi \tag{18.3}$$
3. Let $\psi : C_2 \to C_3$ be another non-constant morphism of smooth curves. Then

for all $P \in C_1$

$$e_{\psi\circ\phi}(P) = e_\phi(P)e_\psi(\phi(P)) \tag{18.4}$$

Corollary 18.2.3.
A map $\phi : C_1 \to C_2$ in unramified iff $\#\phi^{-1}(Q) = \deg\phi \; \forall \; Q \in C_2$

18.3. Frobenius map

Let $\mathrm{char}(k) = p > 0$ and $q = p^n$. For $f(X) \in k[X]$ and let $f^{(q)}$ be the polynomial obtained from f by raising each coefficient of f to the qth power.

If C/k is a curve, $C^{(q)}/k$ is defined to be the curve whose homogenous ideal is generated by $\{f^{(q)} \mid f \in I(C)\}$. Furthermore, there is a natural map

$$\begin{aligned} \phi : C &\to C^{(q)} \\ [X_0 : \cdots : X_n] &\mapsto [X_0^q : \cdots : X_n^q] \end{aligned}$$

Proposition 18.3.1.
Suppose C/k is a curve and $\phi : C \to C^{(q)}$ is the qth power Frobenious morphism.

1. $\phi^*(k(C^{(q)})) = k(C)^{(q)} = \{f \in k(C)\}$
2. ϕ is purely inseparable.
3. $\deg\phi = q$

Corollary 18.3.2.
Every map $\phi : C_1 \to C_2$ which is a morphism of smooth curves over a field of positive characteristic p factors as

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2$$

with $q = \deg_i(\phi)$ where ϕ is the qth power Frobenius and λ is separable.

19. Lecture-7 (24th January, 2023): Weierstrass equation

19.1. Weierstrass equation

Consider

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{19.1}$$

Let $E \subseteq \mathbb{P}^2$ be the variety given by this Weierstrass equation.

Dehomogenize wrt Z and obtain

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{19.2}$$

with $[0 : 1 : 0]$ as a potential point at infinity.

If $a_i \in k$, then E is defined over k.

- If $\mathrm{char}(k) \neq 2$, then substituting y for $1/2(y - a_1x - a_3)$ gives us

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{19.3}$$

- If $\mathrm{char}(k) \neq 2, 3$ then

$$E : y^2 = x^3 - 27c_4x - 54c_6 \tag{19.4}$$

Example 19.1.1.

Definition 19.1.2.
An elliptic curve is a smooth curve in $\mathbb{P}^2$ given by the Weierstrass equation.

Definition 19.1.3.
Δ is called the discriminant of the Weierstrass equation and j is called the j invariant of an elliptic curve.

Let $P = (x_0, y_0)$ be a singular point satisfying the Weierstrass equation $f(x, y)$. Then,

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f}{\partial Y}(P) = 0$$

20. Lecture-8 (31st January, 2023): Group Law

20.1. Group Law and definition of Elliptic Curve

Proposition 20.1.1.
If E is a curve given by the Weierstrass cubic $f(x,y,z)=0$ and L be a line. Then, number of points of $L\cap E$ counted with multiplicity is 3.

Proof. Suppose $P\in L\cap E$. Multiplicity of intersection of $L\cap E$ at P is given by $\dim_{\bar{k}} K[E]_P/L = \dim_{\bar{k}} \bar{k}[X,Y]_{\mathfrak{m}_P}/\langle \tilde{L},\tilde{f}\rangle$ where $\tilde{}$ is the dehomogenisation depending on the affine chart.

Example 20.1.2.
$P=(0,0), L: x=0$. Multiplicity of $L\cap E$ at P equals $\dim_{\bar{k}}[X,Y]_{\mathfrak{m}_P}/\langle Y^2-X^3+X, X\rangle \simeq \dim_{\bar{k}} \bar{k}[Y]/Y^2 = 2$.

If $L': Y-X=0$, then $\dim_{\bar{k}}[X,Y]_{\mathfrak{m}_P}/\langle Y^2-X^3+X-Y, X\rangle \simeq \dim_{\bar{k}} \bar{k}[Y]/\langle Y(Y-Y^2-1)=\dim_{\bar{k}}\bar{k}=1$ since $Y-Y^2-1$ is an unit.

All of this is a special case of Bezout's theorem which is stated after this proof.

Back to the proof.

Suppose $L: aX+bY+cZ=0$.
Case-1: $b\neq 0$ so $O=[0:1:0]\notin L$. Dehomogenize with respect to Y to get $aX+bY+c=0$. For $P\in L\cap E$,

$$\frac{\bar{k}[E]_P}{\langle L,f\rangle} = \frac{[X,\bar{Y}]_{\mathfrak{m}_P}}{\langle f, aX+bY+c\rangle} = \frac{\bar{k}[X,Y]}{\langle g(X)\rangle}(X-X(P))$$

where $g(X)$ is obtained by substituting $Y=-(aX+c)/b$ to f. Therefore $\dim_{\bar{k}}\bar{k}[E]_P/\langle L,f\rangle =$ multiplicity of $X(P)$ as a root of $g(X)$. This implies the number of points of $L\cap E$ with multiplicity is the number of roots of $g(X)$ with multiplicity which is 3.

Case-2: $b=0$

1. Suppose $a\neq 0 \Rightarrow L: X-cZ=0$.
   Multiplicity of $L\cap E$ at O is $\dim_{\bar{k}}\bar{k}[X,Y]_{\mathfrak{m}_O}/\langle \tilde{f}, X-cZ\rangle \simeq \dim_{\bar{k}}\bar{k}=1$.
   For $P\in \mathbb{A}^2\cap E$, multiplicity of $L\cap E$ at P is $\dim_{\bar{k}}\bar{k}[X,Y]_{\mathfrak{m}_P}\langle f, X-cZ\rangle =$

$\dim_{\bar{k}}(\bar{k}[Y]/h)(Y - Y(P))$ with h obtained from f by substituting $X = c$.
Therefore, the total multiplicity is $1 + \#$ roots with multiplicity of $h = 1 + 2 = 3$

2. $L : z = 0$, then $L \cap E = \{0\}$. In the Weierstrass equation, after homogenization, this will mean that just X^3 survives. Therefore, $\dim_{\bar{k}} \bar{k}[X, Z]_{\mathfrak{m}_P}/\langle \tilde{f}, Z\rangle = \dim_{\bar{k}} \bar{k}[X]/\langle X^3\rangle = 3$

This concludes the proof. □

Theorem 20.1.3.
IF F, G are coprime homogenous polynomials in $k[X, Y, Z]$ and $V = \mathcal{V}(F), W = \mathcal{V}(G) \subseteq \mathbb{P}^2$. Then the number of points of $V \cap W$ with multiplicity equals mn where $m = \deg F, n = \deg G$.

20.1.1. Composition Law of E

Suppose $P, Q \in E$ and L be the line passing through P, Q (if $P = Q$, then L is the tangent line at P) and let R be the third point in the intersection of L with E. Let L' be the line joining R and O the point at infinity. L' intersects E at R, O and a third point. We denote this point by $P \oplus Q$

Proposition 20.1.4.
The composition law above makes E into an abelian group, i.e.,

1. If L intersects E in P, Q, R, then $(P \oplus Q) \oplus R = 0$
2. $P \oplus O = P \; \forall \; P$
3. $P \oplus Q = Q \oplus P \; \forall \; P, Q$
4. If $P \in E$, then there exists $-P \in E$ such that $P \oplus (-P) = 0$
5. If $P, Q, R \in E$, then $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$
6. If E is defined over k, then

$$E(k) = \{(x, y) \in k^2 : f(x, y) = 0\} \cup \{0\}$$

is a subgroup of E.

Proof. s □

Notation: Suppose $P \in E$ $[m]P = \begin{cases} 0 \\ P \oplus \cdots \oplus P & , m > 0 \\ -P \oplus \cdots \oplus -P & , m < 0 \end{cases}$

Now, we can explicitly compute the coordinates of the points. Suppose $P = (x_0, y_0) \in E$. Line passing through P and O: $X - x_0 Z$. Dehomogenize with respect to Z to get $X - x_0 = 0$

$$\begin{aligned} f(X,Y) &= Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X - a_6) \\ \Rightarrow X(-P) &= x_0 \\ \Rightarrow Y(-P) &\text{ is another root of } f(Y, x_0) \\ \Rightarrow Y(-P) &= -y_0 - a_1x_0 - a_3 \\ \Rightarrow -P &= (x_0, -y_0 - a_1x_0 - a_3) \end{aligned}$$

Suppose $P_i = (x_i, y_i), i = 1, 2$.

We want to find $P_1 \oplus P_2$'s coordinates.

If $x_1 = x_2$ and $y_1 + y_2 + ax_2 + a_3 = 0$, then $P_1 \oplus P_2 = 0$. Assume that this is not the case. This means that the line passing through P_1 and P_2 does not go through O and thus $L : Y = \lambda x + \nu$. By high school methods,

If $x_1 \neq x_2$, we get

$$\begin{aligned} \lambda &= \frac{y_1 - y_2}{x_1 - x_2} \\ \nu &= \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \end{aligned}$$

If $x_1 = x_2$, we have

$$\begin{aligned} \lambda &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \\ \nu &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \end{aligned}$$

This implies $f(x, \lambda x + \nu)$ has 3 roots say x_1, x_2, x_3. Let $P_3 = (x_3, y_3 = \lambda x_3 + \nu)$

$$\begin{aligned} \therefore f(X, \lambda X + \nu - (X - x_1)(X - x_2)(X - x_3)) &= 0 \\ \Rightarrow x_1 + x_2 + x_3 &= \lambda^2 + a_1\lambda - a_2 \\ \Rightarrow X(P_1 \oplus P_2) &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ Y(P_1 \oplus P_2) &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

Duplication formula: $X([2]P) = \dfrac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$

Example 20.1.5.
$E : Y^2 = X^3 + 17$. Some points on the curve are $P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 23), P_6 = (43, 282), P_7 = (52, 375), P_8 = (5234, 378661)$
$\therefore P_5 = [-2]P_1, P_4 = P_1 - P_3, P_7 = [3]P_1 - P_3.[2]P_1 = \left(\frac{137}{64}, \frac{-2651}{512}\right), P_2 + P_3 = \left(\frac{-8}{9}, \frac{-169}{27}\right)$

The point being that $E(\mathbb{Q}) = \mathbb{Z}P_1 \oplus \mathbb{Z}P_3$ (Mordell-Weil)
$E(\mathbb{Z}) = \{\pm P_1, \ldots, \pm P_8\}$ (Siegel's theorem)

Corollary 20.1.6.
Suppose $f \in \bar{k}(E) = \bar{k}(X, Y)$. Then

$$f \text{ is even } \Leftrightarrow f \in \bar{k}(X)$$

Proof. '$\Leftarrow$' Let $P = (x_0, y_0)$ then $-P = (x_0, -y_0 - a_1x_0 - a_3)$. This implies and element of $\bar{k}(X)$ is even.

'$\Rightarrow$' Suppose $f \in \bar{k}(X, Y)$ is even. Using Weierstrass equation

$$f(x, y) = g(x) + yh(x), g, h \in \bar{k}(X)$$

f even implies $f(x, y) = f(x, -y - a_1x - a_3)$

$$\begin{aligned} \therefore g(x) + yh(x) &= g(x) + h(x)(-y - a_1x - a_3) \\ \Rightarrow (2y + a_1x + a_3)h(x) &= 0 \forall (x, y) \in E \\ \Rightarrow h(x) = 0 \text{ or } a_1 = a_3 &= 0 \end{aligned}$$

In the latter case we have $\Delta = 0 \Rightarrow E = 0 \Rightarrow\Leftarrow$. Therefore, $h(x) = 0 \Rightarrow f(x, y) = g(x) \in \bar{k}(E)$ □

20.2. Group Law for singular Weierstrass equation

Let E be a curve given by the Weierstrass equation E_{ns} = set of non-singular points of E.

If $P \in E$ is a singular point. The multiplicity of $L \cap E$ at P equals $\dim_{\bar{k}} \bar{k}[E]_P/L > 1$. This is because $\bar{k}[E]_P$ is not a DVR and going modulo 1 relation does not give us $\bar{k}$ and thus dimension over $\bar{k}$ is atleast 2.

Law of composition on E_{ns} = same as the one we give to the non-singular Weierstrass equation.

Proposition 20.2.1.
Let E be a curve given by a singular Weierstrass equation. The law of composition makes E_{ns} into an abelian group and,

1. If E has a node, then

$$E_{ns} \to \bar{K}^{\times}$$
$$(x, y) \mapsto \frac{Y - \alpha_1 X - \beta_1}{Y - \alpha_2 X - \beta_2}$$

   is an isomorphism of abelian groups, where $X = \alpha_2 X + \beta_2, Y = \alpha_1 X + \beta_1$

2. If E has a cusp, $Y = \alpha X + \beta$ is a tangent at S, then

$$E_{ns} \to \bar{k}^{\times}$$
$$(x, y) \mapsto \frac{Y - X(S)}{Y - \alpha X - \beta}$$

   is an isomorphism of abelian groups.

Definition 20.2.2.
An elliptic curve is a pair (E, O) where E is a nonsingular curve of genus 1 and $O \in E$. The elliptic curve E is defined over k written E/k if E is defined over k as a curve and $O \in E(k)$.

To make sense of this definition we will have to employ more algebraic geometry as seen in next portion.

21. Lecture-9 (2nd February, 2023): Group Law and more algebraic geometry

21.1. Algebraic geometry

21.1.1. Divisors

Consider the formal linear combination

$$D = \sum_{P \in C} n_P P$$

with $n_P = 0$ for all but finitely many $P \in C$. This formal linear combination is called a divisor of C. CLearly, this forms a free abelian group over the points of C. We denote this group by $\mathrm{Div}(C)$.

The degree of a divisor D is defined as

$$\deg D = \sum_{P \in C} n_P$$

The divisors of degree 0 form a subgroup of

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \deg D = 0\}$$

If C is defined over k, we get a Galois action on $\mathrm{Div}^0(C), \mathrm{Div}(C)$ as follows:

$$\sigma D = \sum_{P \in C} n_P \sigma P$$

Then we say D is defined over k iff $\sigma D = D$ for all $\sigma \in G$. We denote the group of divisors defined over k by $\mathrm{Div}_k(C)$ and similarly $\mathrm{Div}^0_k(C)$

Next, suppose $f \in \bar{k}(C)^\times$. Then we can associate a divisor to this by letting

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$$

This is indeed a divisor from a previous observation that we made.

Notice that if $\sigma \in G$, then

$$\operatorname{div}(\sigma f) = \sigma(\operatorname{div}(f))$$

Or equivalently if $f \in \bar{k}(C)$ then $\operatorname{div}(f) \in \operatorname{Div}_k(C)$.

Since each ord_P is a valuation, the map $\operatorname{div} : \bar{k}(C) \to \operatorname{Div}(C)$ is a homomorphism of abelian groups.

Definition 21.1.1.
A divisor D is called principal divisor if it has the form $D = \operatorname{div}(f)$ for some $f \in \bar{k}(C)^\times$. Two divisors are equivalent $D_1 \sim D_2$ if $D_1 - D_2$ is a principal divisor.

The divisor class group or Picard group of C denoted by $\operatorname{Pic}(C)$ is the quotient of $\operatorname{Div}(C)$ modulo the principal divisors. We let $\operatorname{Pic}_k(C)$ be the subgroup of $\operatorname{Pic}(C)$ fixed by G.

Proposition 21.1.2.
Let C be a smooth curve and let $f \in \bar{k}(C)^\times$.

1. $\operatorname{div}(f) = 0$ if and only if $f\bar{k}^\times$.
2. $\deg(\operatorname{div}(f)) = 0$

Definition 21.1.3.
From the previous definition, it is clear that the principal divisors form a subgroup of $\operatorname{Div}^0(C)$. The quotient of $\operatorname{Div}^0(C)$ by the subgroup of principal divisors is denoted by $\operatorname{Pic}^0(C)$. Similarly, we define $\operatorname{Pic}^0_k(C)$ to be the subgroup of $\operatorname{Pic}^0(C)$ fixed by G.

All the information above can be summarised in the following exact sequence
Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. We have already seen that this induces the two maps

$$\phi^* : \bar{k}(C_2) \to \bar{k}(C_1) \phi_* : \bar{k}(C_1) \to \bar{k}(C_2)$$

Similarly, we define maps of divisor groups as follows:

$$\begin{aligned} \phi^* : \operatorname{Div}(C_2) &\to \operatorname{Div}(C_1) & \qquad \phi_* : \operatorname{Div}(C_1) &\to \operatorname{Div}(C_2) \\ (Q) &\mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P) P & \qquad (P) &\mapsto (\phi(P)) \end{aligned}$$

Extend these maps $\mathbb{Z}$ linearly to arbitrary divisors.

Proposition 21.1.4.
Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves.

1. $\deg(\phi^* D) = (\deg \phi)(\deg D)$ for all $D \in \operatorname{Div}(C_2)$

2. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$ for all $k \in \bar{k}(C_2)^\times$
3. $\deg(\phi_*(D)) = \deg D$ for all $D \in \mathrm{Div}(C_1)$
4. $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$ for all $f \in \bar{k}(C_1)^*$
5. $\phi_* \circ \phi^*$ acts as multiplication by $\deg \phi$ on $\mathrm{Div}(C_2)$
6. If $\psi : C_2 \to C_3$ is another such map, then

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \text{ and } (\psi \circ \phi)_* = \psi_* \circ \phi_*$$

21.1.2. Differentials

Definition 21.1.5.
Let C be a curve. The space of meromorphic differential forms on C, denoted by Ω_C is the $\bar{k}$ vector space generated by symbols of the form dx for $x \in \bar{k}(C)$ modulo the relations :

1. $d(x+y) = dx + dy$ for all $x, y \in \bar{k}(C)$
2. $d(xy) = xdy + ydx$ for all $x, y \in \bar{k}(C)$
3. $dx = 0$ for all $x \in \bar{k}$

Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. The associated function field map $\phi^* : \bar{k}(C_2) \to \bar{k}(C_1)$ induces a map of differentials :

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$
$$\phi^*\left(\sum_i f_i dx_i\right) = \sum_i (\phi^* f_i) d(\phi^* x_i)$$

Proposition 21.1.6.
Let C be a curve.

1. Ω_C is 1-dimensional $\bar{k}(C)$ vector space.
2. Let $x \in \bar{k}(C)$. Then dx is a $\bar{k}(C)$ basis for Ω_C iff $\bar{k}(C)/\bar{k}(x)$ is a finite separable extension.
3. Let $\phi : C_1 \to C_2$ be a non-constant map of curves. Then ϕ is separable iff the map ϕ^* is injective.

Proposition 21.1.7.
Let C be a curve, $P \in C$ and $t \in \bar{k}(C)$ an uniformiser at P.

1. For every $\omega \in \Omega_C$ there exists an unique function $g \in \bar{k}(C)$ depending on ω

and t satisfying

$$\omega = gdt$$

2. Let $f \in \bar{k}(C)$ with $\omega \neq 0$. The quantity

$$\mathrm{ord}_P(\omega/dt)$$

depends on ω and P, independent of the choice of uniformiser t. We call this value the order of ω at P and denote it by $\mathrm{ord}_P(\omega)$.

3. Let $x, f \in \bar{k}(C)$ with $x(P) = 0$ and let $\mathrm{char}(k) = p$. Then,

$$\begin{aligned} &\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1 && \text{if } p = 0 \text{ or } p \nmid \mathrm{ord}_P(x) \\ &\mathrm{ord}_P(fdx) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x) && \text{if } p > 0 \text{ and } p \mid \mathrm{ord}_P(x) \end{aligned}$$

4. Let $\omega \in \Omega_C$ with $\omega \neq 0$. Then $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.

Definition 21.1.8.
Let $\omega \in \Omega_C$. The divisor associated to ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P \in \mathrm{Div}(C)$$

The differential ω is regular or holomorphic if

$$\mathrm{ord}_P(\omega) \geq 0 \quad \forall\, P \in C \tag{21.1}$$

It is nonvanishing if

$$\mathrm{ord}_P(\omega) \leq 0 \quad \forall\, P \in C \tag{21.2}$$

Remark 21.1.9.
If $\omega_1, \omega_2 \in \Omega_C$ are nonzero differentials, then there exists a function $f \in \bar{k}(C)^\times$ such that $\omega_1 = f\omega_2$. Therefore

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$$

Definition 21.1.10.
The canonical divisor class on C is the image in $\mathrm{Pic}(C)$ of $\mathrm{div}(\omega)$ for any non-zero differential $\omega \in \Omega_C$. Any choice in this divisor class is called a canonical divisor.

22. Lecture-10 (7th February, 2023): Riemann-Roch theorem

Definition 22.0.1.
1. A divisor D is positive, denoted by $D \geq 0$ if $n_P \geq 0 \; \forall \; P \in C$.
2. $D_1, D_2 \in \mathrm{Div}(C)$, then $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.
3. For $D \in \mathrm{Div}(C)$

$$\mathcal{L}(D) = \{f \in \bar{k}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}$$
$$\ell(D) = \dim_{\bar{k}} \mathcal{L}(D)$$

Proposition 22.0.2.
Suppose $D \in \mathrm{Div}(C)$

1. If $\deg D < 0$, then $\mathcal{L}(D) = \{0\}$ and $\ell(D) = 0$.
2. $\mathcal{L}(D)$ is finite dimensional over $\bar{k}$.
3. If $D' \in \mathrm{Div}(C)$ and $D \sim D'$, then $\mathcal{L}(D) \cong \mathcal{L}(D')$ and $\ell(D) = \ell(D')$

Proof.
1. If $\mathrm{div}(f) \geq -D$ then $\deg(\mathrm{div}(f)) \geq \deg(-D) = -\deg D$. If $\deg D < 0$, then $\deg(-D) > 0$ and thence no such f exists.
2. For $D' \leq D \Rightarrow \mathcal{L}(D) \subseteq \mathcal{L}(D')$

   Claim: $\dim_{\bar{k}}(\mathcal{L}(D+P)/\mathcal{L}(D)) \leq 1$.

   Proof. Consider the map $\phi_P : \mathcal{L}(D+P) \to \bar{k}$ by $f \mapsto t^{r+1}$ □

□

Theorem 22.0.3 (Riemann-Roch)**.**
Let C be a smooth curve and let K_C be a canonical divisor on C. There is an integer $g \geq 0$ called the genus of C such that for every divisor $D \in \mathrm{Div}(C)$ we have

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

Corollary 22.0.4.
1. $\ell(K_C) = 0$
2. $\deg K_C = 2g - 2$
3. If $\deg D > 2g - 2$, then
$$\ell(D) = \deg D - g + 1$$

Now, we will use this theory to show that every elliptic curve can be written as a plane cubic and conversely any smooth Weierstrass equation is an elliptic curve.

Proposition 22.0.5.
Let E be an elliptic curve defined over k.

1. There exists functions $x, y \in k(E)$ such that the map
$$\phi : E \to \mathbb{P}^2 \text{ is given by } \quad \phi = [x, y, 1]$$
gives an isomorphism of E/k onto the curve given by a Weierstrass equation with $a_i \in k$ satisfying $\phi(O) = [0, 1, 0]$
2. Any two Weierstrass equations for E as in previous part are related by a linear change of variables of the form
$$X = u^2X' + r \qquad Y = u^2Y' + su^2X' + t$$
with $u \in k^\times$ and $r, s, t \in k$
3. Conversely, every smooth cubic curve C given by the Weierstrass equation as in first part is an elliptic curve defined over k with base point $O = [0, 1, 0]$

Corollary 22.0.6.
Let E/k be an elliptic curve with Weierstrass coordinate functions x, y. Then,
$$k(E) = k(x, y) \text{ and } \qquad [k(E) : k(x)] = 2$$

23. Lecture-11 (9th February, 2023): Isogenies

Lemma 23.0.1.
Let C be a curve of genus 1 and let $P, Q \in C$. Then

$$(P) \sim (Q) \Leftrightarrow P = Q \tag{23.1}$$

Proposition 23.0.2.
Let (E, O) be an elliptic curve.

1. For every 0-degree divisor $D \in \mathrm{Div}^0(E)$ there exists an unique point $P \in E$ satisfying
$$D \sim (P) - (O) \tag{23.2}$$
Define
$$\sigma : \mathrm{Div}^0(E) \to E \tag{23.3}$$
to be the map that sends D to its associated P
2. The map σ is surjective.
3. Let $D_1, D_2 \in \mathrm{Div}^0(E)$. Then,
$$\sigma(D_1) = \sigma(D_2) \Leftrightarrow D_1 \sim D_2 \tag{23.4}$$
Thus σ induces a bijection of sets
$$\sigma : \mathrm{Pic}^0(E) \xrightarrow{\sim} E \tag{23.5}$$
4. The inverse to σ is the map
$$\kappa : E \xrightarrow{\sim} \mathrm{Pic}^0(E) \qquad P \mapsto (\text{ divisor class of } (P) - (O)) \tag{23.6}$$
5. If E is given by a Weierstrass equation, then the geometric group law on E and the algebraic group law are the same.

Corollary 23.0.3.

Let E be an elliptic curve and $D \in \mathrm{Div}(E)$. Then D is a principal divisor iff

$$\sum_{P \in E} n_P = 0 \text{ and } \sum_{P \in E} [n_P]P = O \tag{23.7}$$

23.1. Isogenies

24. Lecture-12 (14th February, 2023): Isogenies continued

24.1. Isogenies

25. Lecture-13 (15th February, 2023):

Part III.

Basic Algebraic Geometry

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

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

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

27.2. Zariski topology

Definition 27.2.1.

- 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 27.2.2 (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 27.2.3.
$\mathrm{Spec}(R)$ 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 27.2.4.
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 27.2.5.
$x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$.

Remark 27.2.6.
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 27.2.7.

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

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. □

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

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

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

28.1. Zariski topology contd..

Definition 28.1.1.
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 28.1.2.
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 28.1.3.
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 28.1.4.
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 28.1.5. *Suppose J is maximal wrt not being generated by a cardinal number of generators. Then, J is prime.*

Definition 28.1.6.
A topological space X is said to be irreducible if it cannot be written as the union of proper closed subsets of X

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

Proposition 28.2.1.
The sets $\mathcal{V}(\mathfrak{p})$ are exactly the irreducible components of $\mathrm{Spec}(R)$.

Lemma 28.2.2.
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 28.2.3.
$\mathcal{V}(\mathfrak{p})$ 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 28.2.4.
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 28.2.5 (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 28.2.6.
X^* is also spectral.

Proof. □

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

29.1. Noetherian spaces

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

Proposition 29.1.1.
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 29.1.2.

Definition 29.1.3.

Theorem 29.1.4.
A module M over R is Noetherian iff the module is finitely generated and finitely presented.

Proof. □

Proposition 29.1.5.
The direct sum of projective modules is projective.

Proposition 29.1.6.
The direct product of injective modules is injective.

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

Proposition 29.1.7.
Direct sum of injective modules is injective iff the module is Noetherian.

30. 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 30.0.1 (read this here)**.**
The above mentioned topology is the same as Zariski topology OR the space is spectral.

Remark 30.0.2.
The takeaway point being this is also another way to get a spectral space.

Exercise 30.0.3. *Suppose X is spectral, $Y \subseteq X$ be a quasi-compact open subset. Then, Y is spectral.*

30.1. Localisation

Definition 30.1.1.
A multiplicatively closed set S is one that has the following properties:

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

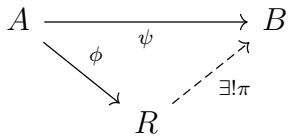
Example 30.1.2. 1. Invertible elements of a ring.

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 30.1.3.
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

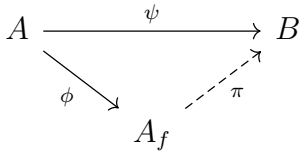
$$A_f = \{ \text{ localisation of } A \text{ at } f\}$$

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

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

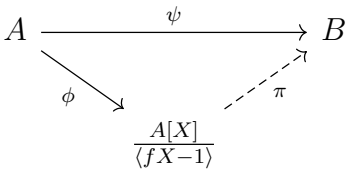
Now, the question is why are the two notions equivalent.



with

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

And,



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

30.1.1. Prime ideals of A_f

Theorem 30.1.4.
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

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

There is a bijection between

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

Say $\mathfrak{P}$ is a prime ideal of A_S. Then, $\mathfrak{P} = \frac{\mathfrak{p}}{s}$ with $\mathfrak{p}$ prime in A.

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

31.1. 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 31.1.1.
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.

31.2. Exact sequences

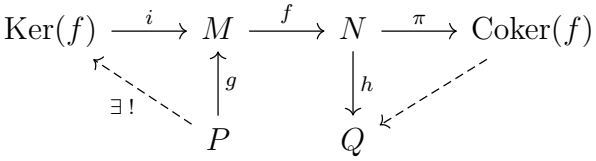
Suppose

$$f : M \to N$$

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 31.2.1.

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

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

Lemma 31.2.2. 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. 1. $\ker f = \mathrm{Im}(0 \to M')$

2. $\mathrm{Im}(g) = \ker(M'' \to 0) = M$

□

Definition 31.2.3.
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 31.2.4.
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

Proof. **Claim**: $\ker(f)_S = \ker(f_S)$
$\subseteq$ is clear since $\frac{f(m)}{s} = 0$. Suppose $\frac{m}{s} \in \ker(f_S) \Rightarrow f(m)/s = 0 \in M_S$. This means that there is a $t \in S$ such that $tf(m) = 0 = f(tm) \Rightarrow tm \in \ker(f) \Rightarrow \frac{tm}{ts} = \frac{m}{s} \in \ker(f)_S$. This gives us " $\supseteq$ ".

Similarly, $\mathrm{Coker}(f)_S = \mathrm{Coker}(f_S)$. This completes the proof. □

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 $M_\mathfrak{m} = 0 \ \forall \ \mathfrak{m} \Rightarrow M = 0$. Take an element $m \in M$ such that $\frac{m}{1} = 0 \in M_\mathfrak{m}$ for each maximal ideal $\mathfrak{m}$ in A. Suppose $\mathrm{Ann}(m) \neq A$, then $\mathrm{Ann}(A) \subsetneq \mathfrak{m}'$ for some maximal ideal $\mathfrak{m}'$. But then we will have $sm = 0$ for some $s \in A\backslash\mathrm{Ann}(m)$ which is a contradiction. Hence, $\mathrm{Ann}(m) = A$ and $m = 0$. This completes the claim.
- 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 $\mathfrak{m}$.

We can summarise in the following theorems

Theorem 31.2.5.
Let M be an A-module and $m \in M$. Then TFAE:

1. $m = 0$.
2. $\frac{m}{1} = 0$ in $M_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of A.
3. $\frac{m}{1} = 0$ in $M_\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$ of A.

Theorem 31.2.6.
Let M be an A-module. Then TFAE:

1. $M = 0$.
2. $M_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p}$ of A.
3. $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ of A.

Theorem 31.2.7.
Let $\phi : M \to N$ be an R-module homomorphism. Then, TFAE:

1. ϕ is injective.
2. $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{m}$ is injective for all prime ideals $\mathfrak{p}$.

3. $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$.

Proof. From the exactness of the sequence as per a proposition mentioned above we have $1 \Rightarrow 2, 1 \Rightarrow 3$. Moreover, $2 \Rightarrow 3$. We wish to show that $3 \Rightarrow 1$. Let $M' = \ker(\phi)$. Then we have the following exact sequence

$$0 \to M' \to M \to N$$

By the proposition above, we have

$$0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$$

exact. This implies $M'_{\mathfrak{m}} = \ker(\phi_{\mathfrak{m}}) = 0$ since $\phi_{\mathfrak{m}}$ is injective by hypothesis. Therefore, $M'_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$. Now, the result follows from previous theorem. □

The same theorem can be repeated with injective replaced with surjective. This leads us thereby to the last conclusion in the points mentioned before these theorems.

Definition 31.2.8.
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 31.2.9.
For sets, these mean injection and surjection but monomorphism and epimorphism need not mean isomorphism in a random category.

32. Lecture-7 (7th February, 2023): Hilbert-Basis Theorem

32.1. Hilbert basis theorem

Definition 32.1.1.
An ideal I is irreducible if

$$I = J \cap K$$

implies $I \supseteq J$ or $I \supseteq K$ (could just say $I = J$ or $I = K$).

Theorem 32.1.2.
In a Noetherian ring, every ideal is finite intersection of irreducible ideals.

Proof. Say S is the collection of ideals that are not finite intersections of irreducible ideals. S is non-empty since maximal ideals are □

Proposition 32.1.3.
If R is Noetherian, then R/I is also Noetherian for any ideal I.

Theorem 32.1.4 (Hilbert Basis theorem)**.**
Let R be a Noetherian ring, then $R[X]$ is also Noetherian.

Proof. □

Definition 32.1.5.
A R-module M is Noetherian iff it satisfies one of the following equivalent conditions:

1. Every submodule N of M is finitely generated.
2. Every collection of submodules has a maximal element.
3. Satisfies a.c.c.

Proposition 32.1.6.
If M_1, M_2 are Noetherian R-modules, then $M_1 \oplus M_2$ is also Noetherian.

Proof. □

Corollary 32.1.7.
If R is Noetherian ring, then R^n is a Noetherian module.

Proposition 32.1.8.
Every finitely generated module on a Noetherian ring is Noetherian.

33. Lecture-8 (8th February, 2023): Affine Varieties

33.1. Zariski topology

Let k be an algebraically closed field.

$\mathbb{A}^n(k) = k^n$ be the affine space.

$k[X_1, \ldots, X_n =: \mathbf{X}]$ be the polynomial ring that is Noetherian by Hilbert basis theorem.

Take an ideal $I \subseteq k[\mathbf{X}]$. We define

$$\mathcal{V}(I) = \{\mathbf{x} := (x_i) \in \mathbb{A}^n : f(\mathbf{x}) = 0 \; \forall \; f \in I\} = \bigcap_{f_1,\ldots,f_r \text{ generates } I} \mathcal{V}(f_i)$$

Properties:

1. If $I \subseteq J \Rightarrow \mathcal{V}(I) \supseteq \mathcal{V}(J)$.
2. If I, J are ideals, then $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J) = \mathcal{V}(IJ)$.
3. If $\{I_\alpha\}_{\alpha \in A}$ is a collection of ideals, then $\mathcal{V}(\sum_{\alpha \in A} I_\alpha) = \bigcap_{\alpha \in A} \mathcal{V}(I_\alpha)$.
4. $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$. Clearly, $\mathcal{V}(I) \supseteq \mathcal{V}(\sqrt{I})$.

The first 3 properties clearly give a topology on the ideals of $k[\mathbf{X}]$ by taking $\mathcal{V}(I)$ to be the closed sets. This topology is called the Zariski topology.

Say, we are given subset S of $\mathbb{A}^n(k)$. We wish to associate an ideal to this subset by defining

$$\mathcal{I}(S) = \{f \in k[\mathbf{X}] : f(\mathbf{x}) = 0\}$$

Properties:

1. It is clearly an ideal. Actually, it is a radical ideal.
2.

$$\begin{aligned} \{\text{ideals in } k[\mathbf{X}]\} &\to \{\text{subsets of } \mathbb{A}^n\} & &\to \{\text{ideals in } k[\mathbf{X}]\} \\ I &\to \mathcal{V}(I) & &\to \mathcal{I}(V(I)) \end{aligned}$$

Clearly, $I \subseteq \mathcal{I}(\mathcal{V}(I)) \Rightarrow \sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(I))$. So, instead of asking whether $I = \mathcal{I}(\mathcal{V}(I))$, it is much more interesting to ask whether $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$

Take an ideal $I \in k[\mathbf{X}]$ and say $\{f_1, \ldots, f_r\}$ generates I. Then, $\mathcal{V}(I)$ is the set of points where all $f_i's$ vanish. Say g vanishes where $f_i's$ vanish. Then, $g \in \sqrt{I} \Rightarrow g^n \in I \Rightarrow g^n = \sum_i r_i f_i$.

Next, consider the ideal J generated by $f_1, \ldots, f_r, gX_{n+1} - 1 \subseteq k[\mathbf{X}, X_{n+1}]$. If $(a_1, \ldots, a_{n+1}) \in \mathcal{V}(J)$, then all $f_i s$ vanish on this point and thus g also vanishes which implies polynomials in J cannot simultaneously vanish and thus $\mathcal{V}(J) = \emptyset$. So, naturally we can ask whether $J = R$ OR $\mathcal{V}(J) = \emptyset \Leftrightarrow J = R$ (a deep theorem, we will prove later). Suppose we have proven this already and proceed further. Take g as before.

Now, this means

$$1 = \sum_i r_i f_i + r_{n+1}(gX_{n+1} - 1)$$
$$g^N = \sum_i s_i f_i + s_{n+1}(g - Y) \text{ for some large value of } N \text{ and } Y = 1/X_{n+1}$$

If we set $G = Y$, then clearly $g^N \sum_i s_i f_i \Rightarrow g^N \in I \Rightarrow g \in \sqrt{I}$. This leads us to the famous Hilbert Nullstellansatz. (This is just a sketch of what will happen, so spare the details for now)

34. Lecture-9 (9th February, 2023): Tensor products

Defined tensor product. Not writing it down. Universal property, blah blah

Theorem 34.0.1.
Suppose $R \to S$ is a ring homomorphism. Then, $R \to S$ is an epimorphism iff $S \otimes_R S = S$

Proof. □

35. Lecture-10 (14th February, 2023): More Tensor products

We have shown that $R \to S$ is a ring epimorphism iff $S \otimes_R S = S$. Therefore, if we localise A wrt T, we know that $A \to A_T$ is an epimorphism iff $A_T \otimes_A A_T = A_T$.

36. Lecture-11 (16th February, 2023):

37. Shaferavich Alg geo rant

This chapter will contain anything that requires justification and also solutions to exercises.

37.1. Schemes

37.1.1. The Spec of a ring

Part IV.

Algebraic Geometry I

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

38.1. Topological properties

Consider a topological space X.

Definition 38.1.1.
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 38.1.2. *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 38.1.3.
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 38.1.4.
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 38.1.5.
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 38.1.6.
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 38.1.7.
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 38.1.8.
A topological space is called Noetherian if set of all closed subsets of X satisfies dcc.

Lemma 38.1.9.
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 38.1.10.
The converse need not be true. Consider $[0, 1]$ covered by $[1/2^n, 1]$.

Lemma 38.1.11.
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 38.1.12.
Locally Noetherian means every point $x \in X$ has a neighbourhood U which is Noetherian wrt subspace topology.

Lemma 38.1.13.
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 38.1.14. *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 38.1.15.
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 38.1.16.
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 38.1.17.
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 38.1.18.
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 38.1.19.
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 38.1.20.
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 $\overline{\{x\}} = X$)

38.2. 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 38.2.1.
$\mathrm{Spec}(A)$ 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.

□

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

39.1. Zariski topology contd..

Theorem 39.1.1 (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 39.1.2.
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

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

□

39.2. Affine schemes

Definition 39.2.1.
$\mathrm{Spec}(A)$ will be called an affine "scheme" (we will see this properly later on).

Definition 39.2.2.
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 39.2.3.
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 39.2.4.
If $X = \mathrm{Spec}(A)$. A regular function on X is a regular map from X to $\mathrm{Spec}(\mathbb{Z}[t])$.

Proof. □

Remark 39.2.5.
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 39.2.6.
Every affine scheme has a closed point.

Proof. Every commutative ring has a maximal ideal. □

Definition 39.2.7.
Open in affine is called quasi-affine.

Example 39.2.8.
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.

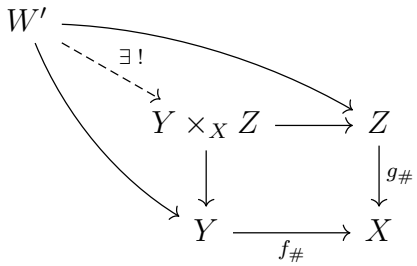
Exercise 39.2.9. *Let $A = k[X_1, X_2, \ldots], B = A_{\mathfrak{m}}, X = \mathrm{Spec}(B)\backslash\mathfrak{m}, \mathfrak{m} = \langle X_1, X_2, \ldots, \rangle$. Claim is that X has no closed point.*

39.2.1. 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 39.2.10.
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 39.2.11.
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

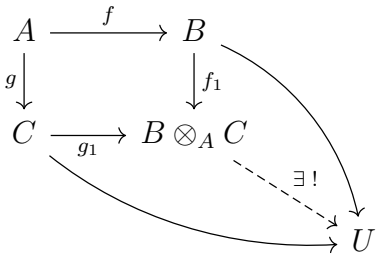
following diagram due to the nature of tensor product

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

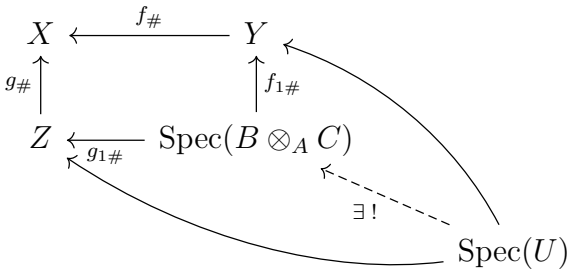
Now, let $W = \mathrm{Spec}(B \otimes_A C)$ and we claim that this satisfies the universal property of fibre product. Apply $\mathrm{Spec}(-)$ functor to the diagram to get

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

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



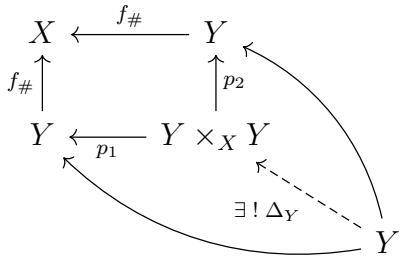
Again, apply the $\mathrm{Spec}(-)$ functor.



This completes the proof. □

40. 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 40.0.1.
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 40.0.2.
Δ_Y is a closed immersion.

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

Example 40.0.3.
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 40.0.4.
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 40.0.5.
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 40.0.6.
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.

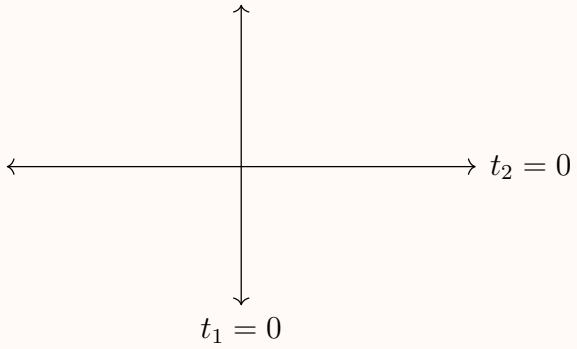
□

Remark 40.0.7.
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 40.0.8 (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 40.0.9 (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 40.0.10.
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 40.0.11.

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

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 40.0.12.
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 40.0.13.
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.

40.1. 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

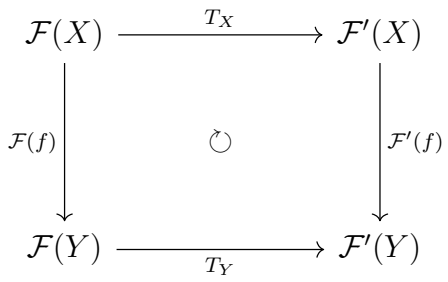
$$\mathrm{ob}(\mathcal{C}) = \mathrm{ob}(\mathcal{C}^{\mathrm{op}})$$

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

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

41.1. Category theory contd..

41.1.1. 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 41.1.1.
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.

41.1.2. Products and Co-products

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

41.2. 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 41.2.1 (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 41.2.2.
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. □

41.2.1. 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 41.2.3.

1. Take $\mathcal{C}, \mathcal{D}$ to be the category $\mathbf{Mod}_R$ of R-modules. Define the functors

$$\begin{aligned} F &: \mathcal{C} \to \mathcal{D} & G &: \mathcal{D} \to \mathcal{C} \\ F(A) &= A \otimes_R N & G(B) &= \mathrm{Hom}_R(N, B) \end{aligned}$$

   Consider $\mathrm{Hom}_R(A \otimes_R N, B)$ and $\mathrm{Hom}_R(A, \mathrm{Hom}_R(N, B))$. These are both in bijective correspondence, in fact they are isomorphic as R-modules. Hence, (F, G) is an adjoint pair. This is also called the Hom-tensor adjunction.

2. (F, G) with F the free functor and G the forgetful functor is also an adjoint pair.

Proposition 41.2.4.
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 41.2.5.
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 41.2.6.
It is an additive category such that every map $f : X \to Y$ has a kernel and a cokernel.

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

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

Definition 42.0.1.
M is flat if

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

Definition 42.0.2.
M is faithfully-flat if M is flat and

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

Definition 42.0.3.
M is projective if it is a direct summand of a free A-module. Or equivalently,

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

Lemma 42.0.4.
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. $1 \Rightarrow 2$ is obvious. $2 \Rightarrow 3$ is a local property. $3 \Rightarrow 4$ is done in commutative algebra. $4 \Rightarrow 1$: Note that $4 \Rightarrow 3 \Rightarrow 2$. So we just prove that $2 \Rightarrow 1$. Thus, enough to show that

$$\begin{aligned} \mathrm{Ext}^i_A(M, N) = 0 & \qquad \forall\ N \forall\ i > 0 \\ \Leftrightarrow \mathrm{Ext}^i_A(M, N)_{\mathfrak{m}} = 0 & \qquad \forall \mathfrak{m} \text{ maximal ideals} \\ \Leftrightarrow \mathrm{Ext}^i_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}, N_{\mathfrak{m}}) = 0 & \end{aligned}$$

This completes the proof. □

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

Definition 42.0.5.
A is called separable over k if $A \otimes_k k'$ is reduced for all field extensions k'/k.

Lemma 42.0.6.
A is separable over k iff every finitely generated subalgebra is separable over k.

Proposition 42.0.7.
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. $(1 \Rightarrow 2)$

$$\bar{A} = \prod_{i=1}^{n} A_{\mathfrak{m}_i} = \prod_{i=1}^{n} \bar{k}$$

$(2 \Rightarrow 3)$

$$\frac{A}{\mathrm{Nil}(A)} = \prod_{i=1}^{n} k_i$$

where k_i is finite field extension of k.

$\bar{A}$ is reduced $\Rightarrow \mathrm{Nil}(A) = 0 \Rightarrow A \simeq \prod_{i=1}^{n} k_i$.

Now, say that A is a finite field extension of k. Say $A = k'$. We have the following inclusions

$$k \hookrightarrow k'' \hookrightarrow k'$$

where k' is the maximal purely inseparable extension of k inside k'. Need to show that $k'' = k$.

Can make

$$k'' = \frac{k[t]}{t^{p^n} - \alpha}, \alpha \in k$$

Therefore

$$k' \otimes_k \bar{k} = \frac{\bar{k}[t]}{t^{p^n} - \beta^{p^n}} = \frac{\bar{k}[t]}{(t - \beta)^{p^n}}$$

for some $\beta \in \bar{k}$. Since the last quotient is not reduced therefore $k'' = k$.

$(3 \Rightarrow 4)$ done in comm. alg.

$(4 \Rightarrow 1)$

$$\begin{aligned} \varphi : A \times A &\to k \\ (w, w') &\mapsto \mathrm{Tr}_{A/k}(ww') \end{aligned}$$

is non-degenerate.
Let $\{w_1, \ldots, w_n\}$ be a k-basis of A.
Consider $B = (\mathrm{Tr}(w_i w_j))$ and $\mathrm{disc}_k(A) = \det(B) \neq 0 \Rightarrow \mathrm{disc}_{\bar{k}}(\bar{A}) \neq 0$.
Suppose that $\mathrm{Nil}(\bar{A}) \neq 0$. Suppose $\{w_1, \ldots, w_m\}$ be a $\bar{k}$-basis of $\bar{A}$. Extend this to a basis $\{w_1, \ldots, w_m, w_{m+1}, \ldots, w_n\}$ of A such that $w_i w_j$ is nilpotent for all i, j. This implies $\det(\mathrm{Tr}(w_i w_j)) = 0$ which is a contradiction. Therefore $\mathrm{Nil}(\bar{A}) = 0$. □

42.1. Kahler Differentials

Some reference materials.

- advanced1 advanced2 advanced3
- basic
- Matsumura book on Commutative algebra and Commutative ring theory
- Chapter 4 of T.A. Springer's Linear Algebraic Groups.

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

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

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 42.1.1.
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 42.1.2.
$\mathrm{Der}_k(A, -)$ is a representable functor.

Proof. □

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

43.1. Differentials and Derivations

Theorem 43.1.1.
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. Take $\Omega^1_{A/k}$ to be the free A-module generated by symbols $\{da : a \in A\}$ modulo the relations $d(a+b) - d(a) - d(b) = 0$ and $d(ab) = ad(b) + bd(a)\ \forall\ a, b \in A$. □

Definition 43.1.2.
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 43.1.3.
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.

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

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

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

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.

$$a \otimes a' = (a \otimes 1)(-a' \otimes 1 + 1 \otimes a') + aa' \otimes 1$$

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

□

□

Corollary 43.1.4.

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

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

Definition 43.1.5.
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 43.1.6.
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 43.1.7.
We say that A is smooth (resp. unramified, étale) if it is formally smooth (unramified, étale) and finite type over k.

Exercise 43.1.8. $A = k[X_1, \ldots, X_n], \Omega'_{A/k} = ?$
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 43.1.9.
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.

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

Lemma 44.0.1.
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 44.0.2. *Suppose K/k be a finite separable extension. We claim that this extension is formally unramified.*

Lemma 44.0.3.
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 44.0.4.
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 44.0.5.
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 44.0.6 (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

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

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

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

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

Example 44.0.8.
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,

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

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

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

contd..

Theorem 45.0.1 (Second fundamental theorem of module of differentials)**.** Let $I = \ker(A \twoheadrightarrow B)$. Then, there exists an exact sequence

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

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

Proof. Suffices to show that for any B-module M, the sequence

$$\mathrm{Hom}_B(\Omega^1_{B/k}, M) \xrightarrow{\alpha^*} \mathrm{Hom}_B(\Omega^1_{A/k} \otimes_A B, M) \xrightarrow{\delta^*} \mathrm{Hom}_B(I/I^2, M) \qquad (*)$$

is exact.
Well-definedness of δ:

$$\begin{aligned}
\delta(ab) &= d_{A/k}(ab) \otimes 1 \\
&= (a d_{A/k}(b) + b d_{A/k} a) \otimes 1 \\
&= a d_{A/k} b \otimes 1 + b d_{A/k} \otimes 1 \\
&= d_{A/k} b \otimes g(a) + d_{A/k} \otimes g(b) \text{ since} \\
&= 0 + 0 \\
&= 0
\end{aligned}$$

Now, we have

$$\mathrm{Der}_k(B, M) \xrightarrow{\alpha^*} \mathrm{Hom}_B(\mathrm{Der}_k(A, M) \xrightarrow{\delta^*} \mathrm{Hom}_B(I/I^2, M) \qquad = (*)$$

Take $D \in \mathrm{Der}_k(A, M)$, then $D(a) = 0 \; \forall \; a \in I$. Since,

$$\begin{array}{ccc}
A & \longrightarrow\!\!\!\!\!\rightarrow & B \\
\downarrow & & \\
M & &
\end{array}$$

Therefore there exists $D' \in \mathrm{Der}_k(B, M)$ such that $D' \circ g = D$. Thus, sequence is exact.

Now, assume that B is formally smooth over k. Look at the exact sequence of B-modules which is a square 0 extension of B.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I/I^2 & \longrightarrow & A/I^2 & \xrightarrow{g'} & B & \longrightarrow & 0 \\ & & & & & \nwarrow^{\exists\, h} & \uparrow{\scriptstyle \mathrm{id}} & & \\ & & & & & & B & & \end{array}$$

This implies the existence of a k-algebra homomorphism $h : B \to A/I^2$ such that $g \circ h = \mathrm{id}_B$. Now, consider the map

$$h \circ g' : A/I^2 \to A/I^2$$

that kills I/I^2 so that $g'(1 - hg') = 0$.
Let $D' = 1 - hg' : A/I^2 \to A/I^2$. Check that this is a k-derivation of A/I^2.
Let $\psi \in \mathrm{Hom}_B(I/I^2, M)$ and consider the maps

$$D := A \longrightarrow A/I^2 \xrightarrow{D'} A/I^2 \xrightarrow{\psi} M$$

Since D' is a derivation, check that $D \in \mathrm{Der}_k(A, M)$. This means we get an A-linear map $\varphi : \Omega^1_{A/k} \to M$ which is equivalent to getting a map $\varphi : \Omega^1_{A/k} \otimes_A B \to M$ such that $\delta * (\phi) = \psi$.
Finally, take $M = I/I^2$ and $\psi = \mathrm{id}$.
$\Rightarrow$ $\exists$ a map from $\varphi : \Omega^1_{A/k} \to I/I^2 \Leftrightarrow \varphi : \Omega^1_{A/k} \otimes_A B \to I/I^2$ and $\varphi \circ \delta = \mathrm{id}_{I/I^2}$.
Finally,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I/I^2 & \xrightarrow{\delta} & \Omega^1_{A/k} \otimes_A B & \longrightarrow & \Omega^1_{B/k} & \longrightarrow & 0 \\ & & & \underset{\varphi}{\curvearrowleft} & & & & & \end{array}$$

or the sequence splits. This concludes the proof. □

Corollary 45.0.2.
Let $B = k[X_1, \ldots, X_n]/\langle f_1, \ldots, f_r\rangle$. Thus,

$$\Omega^1_{B/k} = \frac{B d\bar{x}_1 + \cdots + B d\bar{x}_n}{\langle df_1, \cdots, df_r\rangle}$$

with $df_i = \sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j}$ modulo I^2.

Corollary 45.0.3.
Suppose $k \xrightarrow{f} A \xrightarrow{g} \!\!\!\rightarrow B$ are k-algebra homomorphisms such that A, B are

formally smooth over k. Then,

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

Definition 45.0.4. 1. Let $k \xrightarrow{f} A$ be a ring homomorphism. We say that A is unramified over k if it is formally unramified and of finite type.

2. Let $q \in \mathrm{Spec}(A)$. Then, we say that A is unramified over k at q if there exists $g \in A \backslash k$ such that the map $f : K \to A_g$ is unramified.

3. We say that A is locally unramified over k if it is unramified at every $q \in \mathrm{Spec}(A)$.

The question is whether the $1, 3$ conditions are equivalent. $1 \Rightarrow 3$ is known. So we need to check if $3 \Rightarrow 1$. Suppose that for all $q \in \mathrm{Spec}(A)$ there exists $g \notin q$ such that $k \to A_g$ is unramified. Let $U_q = \mathrm{Spec}(A_g)$.
Since X is locally unramified, we must have $X = \bigcup_q U_q$ but remember that X is spectral and thus quasi-compact. This implies that there is a finite subcover $X = \bigcup_{i=1}^{n} U_{q_i} \Rightarrow A = \langle g_1, \ldots, g_n \rangle \Rightarrow A$ is of finite type over k.

Why is $\Omega^1_{A/k} = 0$?

Notice that $\Omega^1_{A_g/k} = 0$ and we have an exact sequence

$$\Omega^1_{A/k} \otimes_A A_g \longrightarrow \Omega^1_{A_g/k} \longrightarrow \Omega^1_{A_g/A} \longrightarrow 0$$

But $\Omega^1_{A_g/A}$ is formally étale and is therefore 0. This transforms the above sequence to

$$0 \longrightarrow \Omega^1_{A/k} \otimes_A A_g \longrightarrow \Omega^1_{A_g/k} \longrightarrow 0$$

Hence, $(\Omega^1_{A/k})_g = \Omega^1_{A_g/k}\ \forall\ g \Rightarrow \Omega^1_{A/k} = 0$. This finishes the proof.

Proposition 45.0.5. 1. Unramified maps are preserved under base change.

2. Unramified maps are preserved under composition.

3. Principal localisations are unramified.

4. Any surjection is unramified.

Proof. Let us prove 3. Look at

$$\begin{array}{ccc} k & \xrightarrow{f} & A \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g'} \\ B & \xrightarrow[f']{} & A \otimes_k B = C \end{array}$$

More generally, we have

Lemma 45.0.6.
$\Omega^1_{C/B} \simeq \Omega^1_{A/k} \otimes_k B$

Proof. Look at the maps as a consequence of first fundamental exact sequence

$$\Omega^1_{A/k} \longrightarrow \Omega^1_{C/k} \twoheadrightarrow \Omega^1_{C/B}$$

This gives the map $\Omega^1_{A/k} \otimes_k B \xrightarrow{\alpha} \Omega^1_{C/B}$. Now, we wish to construct an inverse map $\Omega_{C/B} \to \Omega^1_{A/k} \otimes_k B$. Look at the map $d_{A/k} : A \to \Omega^1_{A/k}$. This gives a map

$$\begin{aligned} d' : C = A \otimes_k B &\to \Omega^1_{A/k} \otimes_k B \\ a \otimes b &\mapsto d_{A/k} a \otimes b \end{aligned}$$

Check that d' is a B-derivation. This implies the existence of a map $\beta : \Omega^1_{C/B} \to \Omega^1_{A/k} \otimes_k B$. Check that $\alpha \circ \beta = \beta \circ \alpha = \mathrm{id}$. The proof is complete. □

□

Lemma 45.0.7.
Let $f \xrightarrow{f} A$ be a finite type morphism. Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Then, A is unramified over k at $\mathfrak{p}$ if $\Omega^1_{A/k} \otimes_A k(\mathfrak{p}) = 0$ where $k(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$.

Proof. It suffices to show that $(\Omega^1_{A/k})_{\mathfrak{p}} = 0$ since A is of finite type. We can deploy Nakayama lemma to conclude what we want. We just need to check that localisation of finitely generated implies finitely generated. □

46. Lecture-9 (6th February, 2023): Differentials

46.1. Differentials contd...

Recall that given a ring homomorphism $k \xrightarrow{A}$, A is unramified iff A is of finite type and $\Omega^1_{A/k} = 0$.

Also, for a finite type algebra A, if $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $\Omega^1_{A/k} \otimes_A k(\mathfrak{p}) = 0$ then A is unramified at $\mathfrak{p}$.

In particular, if $\Omega^1_{A/k} \otimes_A k(\mathfrak{p}) = 0 \ \forall \mathfrak{p} \in \mathrm{Spec}(A)$, then A is unramified.

Lemma 46.1.1. 1. Say A is a commutative ring and $I \subseteq A$ is a finitely generated ideal such that $I = I^2$. Then there exists an idempotent $e \in A$ such that $I = \langle e \rangle$.

2. $A/I = A_{e'}$ where $e'(1-e) = 0$.

3. $\mathcal{V}(I)$ is open in $\mathrm{Spec}(A)$.

Proof. Since $I = I^2$ and I is f.g. then Nakayama lemma implies the existence of an $a \in I$ such that $(1+a)I = 0$. Set $f = 1 + a$. Then $f^2 = ff = f(1+a) = f + af = f$.

Next, take $e' = f$ and $e = 1 - f$. Then $\forall\ b \in I$ we have $b = (1-f)b = eb \Rightarrow I = \langle e \rangle$.

In particular, the map

$$A \to \frac{A}{\langle e \rangle} \times \frac{A}{\langle e' \rangle}$$

is an isomorphism. This helps us conclude that $A/\langle e \rangle = A_{e'}$.

And, $V(I) = \mathrm{Spec}(A/I) = \mathrm{Spec}(A_{e'}) \hookrightarrow \mathrm{Spec}(A)$ is open. □

Corollary 46.1.2.
If $k \xrightarrow{f} A$ is unramified, then the diagonal map $\Delta_X : X \hookrightarrow X \times_Y X$ is a closed and open immersion where $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(k)$.

Proof. Recall that by definition $\Omega^1_{A/k} = I/I^2$ where I is the ideal of X inside $X \times_Y X$. The module of differential is of f.g. since A is of finite type.

Red Flag: I need not be f.g. as required in our previous lemma. So, WE HAVE TO change the definition of unramified by replacing finitely presented instead of finite type. So, work with this definition.

Working with the new definition, we know that $\Omega^1_{A/k} = 0 \Rightarrow I = I^2$ and hence from previous lemma, we know that this immersion is open. □

Lemma 46.1.3.
Let $(A, \mathfrak{m})$ be a local ring which is a k-algebra for some field k such that $A/\mathfrak{m} = k$. Then, $\mathfrak{m}/\mathfrak{m}^2 \simeq \Omega^1_{A/k} \otimes_A k$

Proof. We have an exact sequence

$$0 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \Omega^1_{A/k} \otimes_A k \longrightarrow \Omega^1_{k/k} \longrightarrow 0$$

Here, k sits inside A and acts on A as well, hence the sequence splits and is formally smooth. Now, using a result from before, we know that $\Omega^1_{k/k} = 0$ and hence the proof is complete. □

Lemma 46.1.4.
Suppose A is as in prev. lemma such that A is essentially of finite type (localisation of a finite type) over k. Then, $\Omega^1_{A/k}$ is a free A-module of rank$= \dim(A)$ iff A is a regular ring.

Proof. ($\Rightarrow$) By previous lemma, $\mathfrak{m}/\mathfrak{m}^2$ is free k-module of rank $n = \dim(A)$. Now apply Nakayama to observe that $\mathfrak{m}$ is generated by n generators which is the minimal number required. Hence, A is regular.
Caution: Here, $\mathfrak{m}$ is f.g. requires Noetherian-ness which is guaranteed by the essentially finite-ness.

($\Leftarrow$) Suppose A is regular. Therefore $\mathfrak{m} = \langle x_1, x_2, \ldots, x_n \rangle$ where $n = \dim A$. By previous lemma, $\dim_k(\Omega^1_{A/k} \otimes_A k) = n$.

Let K be the quotient field of A (makes sense because a regular local ring is integral domain). This implies $\dim_K(\Omega^1_{K/k}) = \dim_K(\Omega^1_{A/k} \otimes_A K) = tr.\deg_k(K) = \dim(A) = n$.

PLEASE STOP: The third equality is because of Noether Normalisation theorem. The second equality is some other very non-trivial fact. Just take it for granted for the time being. We will justify it later.
Detour:

Lemma 46.1.5.
Let A be a local integral domain with fraction field K and residue field k. Let M be a f.g. A-module such that $\dim_k(M \otimes_A k) = \dim_K(M \otimes_A K) = n < \infty$. Then, M is a free module of rank n.

Proof. By Nakayama, can find a surjection $\phi : F = A^n \twoheadrightarrow M$. Let $N = \ker(\phi)$. This gives us the exact sequence

$$0 \longrightarrow N \longrightarrow F \xrightarrow{\phi} M \longrightarrow 0$$

which implies

$$0 \longrightarrow N_K \longrightarrow F_K \xrightarrow{\phi} M_K \longrightarrow 0$$

is exact.

We know that $F_k \to M_K$ is a surjection of vector spaces of same dimension (n). Hence, $N_K = 0$. But, N is torsion free therefore $N \hookrightarrow N_K = 0$. □

The proof is now complete using this lemma. □

Corollary 46.1.6.
If $\Omega^1_{A/k} = 0$, then $A = k$.

Lemma 46.1.7.
Let $k \hookrightarrow L$ be an algebraic extension of fields which is separable. Then, L/k is formally unramified.

Proof. Can assume that L/k is finite, and

Lemma 46.1.8.
If $A = \varinjlim_{i \in I} A_i \Rightarrow \Omega^1_{A/k} = \varinjlim_{i \in I} \Omega^1_{A_i/k}$

Proof. □

Can choose a primitive element $\alpha \in L$. Let $f(X)$ be the minimal polynomial of $\alpha \in k[X]$ such that $f(\alpha) = 0$ and $f'(\alpha) \in L^\times$. Now, write $A = k[X]$ and $I = \langle f(X) \rangle \in A \Rightarrow L = k[X]/\langle f(X) \rangle$. By the second fundamental exact sequence, we get that

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

But $\Omega^1_{A/k} \otimes_A L = L d\bar{X}$

And, $\delta(f) = \dfrac{\partial}{\partial X} f|_L d\bar{X} = f'(\alpha) d\bar{X}$. This implies δ is an isomorphism (takes basis to basis). $\Rightarrow \Omega^1_{L/k} = 0$

□

47. Lecture-10 (8th February, 2023): Unramified morphisms

Recall the lemma

Lemma 47.0.1.
If k'/k is an algebraic separable field extension, then k'/k is formally unramified.

Proposition 47.0.2.
Let k be a field and A/k an unramified k-algebra. Then, A is a finite product of finite separable field extensions of k.

Lemma 47.0.3.
A is finite type over k.

Remark 47.0.4.
We can replace k by $\bar{k}$ since basis goes to basis.

Proof. It suffices to show that $\dim(A) = 0$ since it is Noetherian and $\dim(A) = 0$ which implies Artinian. (all primes are maximal ideal and use some ideas about minimal primes stuff + CRT) to conclude. LOTs of details went over my head. Anyway, assume A has one prime ideal and complete.

Now let us show $\dim(A) = 0$. Suppose $\dim(A) > 0$, i.e., there is a maximal ideal $\mathfrak{m}$ such that $\mathrm{ht}(\mathfrak{m}) > 0 \Leftrightarrow \dim(A_{\mathfrak{m}}) > 0$. But, we are given $\Omega^1_{A_{\mathfrak{m}}/k} = 0$. But from corollary in last class, $A_{\mathfrak{m}} = k \Rightarrow\Leftarrow$. (The conditions are satisfied due to Hilbert Nullstellansatz). □

Proof of proposition. Using the lemma, just apply one of the 4 equivalent conditions of separability and the corollary in previous class. □

Lemma 47.0.5.
Let $f : k \to A$ be a ring homomorphism and let $\mathfrak{q} \in \mathrm{Spec}(A) = X$ be a prime. Let $\mathfrak{p} = f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(k) = Y$. Assume that f is unramified at $\mathfrak{q}$. Then,

1. $\mathfrak{p}A_{\mathfrak{q}} = \mathfrak{q}A_{\mathfrak{q}}$
2. $k(\mathfrak{q})$ is a finite separable extension of $k(\mathfrak{p})$

Proof. Since $k \to A$ is unramified at $\mathfrak{q}$, it follows that there exists a $g \in A \backslash \mathfrak{q}$ such that $k \to A_g$ is unramified. In particular, we can assume that A/k is unramified. This means that $k(\mathfrak{p}) \to k(\mathfrak{p}) \otimes_k k(\mathfrak{p}) =: B$ is also unramified as it is just a base change. But this tensor product is still finite type and by previous proposition B is a product of k_i with k_i/k finite separable field extension. One of these $k_i s$ must be $k(\mathfrak{q})$. Therefore, (2) is proven. (1) also follows from this. □

Proposition 47.0.6.
Let $f : k \to A$ be a finite type ring extension and let $\mathfrak{q} \in X = \mathrm{Spec}(A)$ and $\mathfrak{p} = f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(k)$. Suppose

1. $\mathfrak{p}A_\mathfrak{q} = \mathfrak{q}A_\mathfrak{q}$
2. $k(\mathfrak{q})$ is a finite separable extension of $k(\mathfrak{p})$

Then, f is unramified at $\mathfrak{q}$.

Proof. We need to show that $existsg \in A\backslash\mathfrak{q}$ such that $\Omega^1_{A_g/k} = 0$. For this, it suffices to show that $\Omega^1_{A_\mathfrak{q}/k} = 0$ since $\Omega^1_{A/k}$ is a f.g. A-module and use result from previous class (if stalk at a point is 0, then it must be globally 0).

Let us prove $B := \Omega^1_{A_\mathfrak{q}/k} \otimes_k k(\mathfrak{p}) = 0$.
We know that $\Omega^1_{B/k(\mathfrak{p})} = \Omega^1_{A_\mathfrak{q}/k} \otimes_k k(\mathfrak{p})$. Hence, we can assume that B is a localisation if a finite type k-algebra where k is a field. In this case, our hypothesis says that B is a finite separable field extension of k. By the lemma we recorded in the beginning, we have B is unramified. This completes the proof. □

Thus, we have a characterisation of a map being unramified at a point. Let us record it in the following theorem

Theorem 47.0.7.
Let $f : k \to A$ be a finite type ring extension and let $\mathfrak{q} \in X = \mathrm{Spec}(A)$ and $\mathfrak{p} = f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(k)$. Then,

1. $\mathfrak{p}A_\mathfrak{q} = \mathfrak{q}A_\mathfrak{q}$
2. $k(\mathfrak{q})$ is a finite separable extension of $k(\mathfrak{p})$

if and only if f is unramified at $\mathfrak{q}$.

Definition 47.0.8.
Let $f : k \to A$ be a ring homomorphism. Say $\mathfrak{p} \in \mathrm{Spec}(A)$, then we say f is quasi-finite at $\mathfrak{p}$ if $\mathrm{Spec}(A \otimes_k k(\mathfrak{p}))$ is finite.

We say f is quasi finite if it is so at every point of Y.

To understand it better, consider $k \xrightarrow{f} A$ and $X \xrightarrow{f} Y$. Then, for $y \in Y$ look at $f^{-1}(y)$. The ring $A \otimes_k k(\mathfrak{p})$ is just $A/\mathfrak{p}A$. Therefore the $\mathrm{Spec}(A \otimes_k k(\mathfrak{p}))$ is just the prime ideals containing $\mathfrak{p}$. Set theoretically, this is just the fiber of y under f.

Corollary 47.0.9.
Every finite morphism is quasi-finite.

Proof. □

Corollary 47.0.10.
An unramified morphism is quasi-finite.

Proof. To check this at point $\mathfrak{p}$, we can replace k by $k(\mathfrak{p})$ and do base change. Now, the result follows from the proposition proved today. □

PLEASE READ Artinian Rings, Integral extensions, minimal primes business

48. Lecture-11 (13th February, 2023): Smoothness

48.1. Dimension Theory

For an affine scheme X and a point $x \in X$, we let

$$\dim_x(X) := K\dim(\mathcal{O}_{X,x})$$

where $\mathcal{O}_{X,x}$ is the localisation of A at $\mathfrak{p}$ if $X = \mathrm{Spec}(A)$ and $x = \{\mathfrak{p}\}$

From now on we will assume that our rings to be Noetherian.

Recall that if A is a Noetherian ring, then

$$K\dim = \sup\{n \mid \exists \text{ a chain of prime ideals } \mathfrak{p}_0 \subsetneq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \text{ of length } n\}$$

Also, $\dim(X) := \dim(A)$ if $X = \mathrm{Spec}(A)$
If $\mathfrak{p} \in X$, then

$$\mathrm{ht}(\mathfrak{p}) = K\dim(A/\mathfrak{p})$$

We also defined co-height of $\mathfrak{p}$ as

$$\mathrm{co}-\mathrm{ht}(\mathfrak{p}) = K\dim(A_{\mathfrak{p}})$$

Note that $\mathrm{ht} + \mathrm{co} - \mathrm{ht} \leq \dim(A)$

Theorem 48.1.1.
Let A be an integral domain which is of finite type over a field. Then,

1. $\dim(A) = tr.\deg(\mathrm{Frac}(A)/k)$
2. $\forall\ \mathfrak{p} \in \mathrm{Spec}(A)$ we have $\mathrm{ht}(\mathfrak{p}) + \mathrm{co.ht}(\mathfrak{p}) = \dim(A)$

Proof can be seen in the commutative algebra part of the notes.
Now, for any ideal $I \subseteq A$, we define height of I as

$$\mathrm{ht}(I) = \inf\{\mathrm{ht}(\mathfrak{p}) \mid I \subseteq \mathfrak{p}\}$$

Theorem 48.1.2 (Krull dimension theorem)**.**
Suppose there exists $f_1, \ldots, f_r \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime if $I =$

$\langle f_1, \ldots, f_r \rangle$. Then,

$$\operatorname{ht}(\mathfrak{p}) \leq r \tag{48.1}$$

Moreover, if $f_1, \ldots, f_r$ is a regular sequence, then

$$\operatorname{ht}(I) = r \tag{48.2}$$

Corollary 48.1.3.
The height of an ideal is always finite.

Proof. Since the ring is Noetherian, therefore every ideal is f.g and hence by previous theorem $\operatorname{ht}(I) < \infty$. □

Corollary 48.1.4.
If A is semi-local, then $\dim(A) < \infty$

Proof. □

Remark 48.1.5 (due to Nagata)**.**
A Noetherian ring in general might not have finite dimension. For example, take $A = k[X_1, X_2, \ldots]$. Choose a sequence of integers (positive) $m_1 < m_2 < \cdots$ such that $m_{i+1} - m_i > m_i - m_{i-1}\ \forall\ i$

Now, define $\mathfrak{p}_i = \langle X_{m_i}, X_{m_i+1}, \ldots, X_{m_{i+1}} \rangle$

Take $S = \bigcup \mathfrak{p}_i \subseteq A$ and let $B = S^{-1}A$.

Clearly, $\operatorname{ht}(\mathfrak{p}_i) = m_{i+1} - m_i$. This implies $\dim(B) = \infty$.

Remains to be shown that B is Noetherian. (Noetherian local ring has finite Krull dimension, and some other result)

Proposition 48.1.6.
If $\operatorname{ht}(\mathfrak{p}) = r$, then there exists $f_1, \ldots, f_r \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime of $\langle f_1, \ldots, f_r \rangle$.

Definition 48.1.7.
IF A is local and $\mathfrak{m}$ is the minimal prime of $\langle f_1, \ldots, f_r \rangle$ such that $\dim(A) = r$, then $\{f_1, \ldots, f_r\}$ is called a system of parameters of A.

Proposition 48.1.8.
$\dim(A[X_1, \ldots, X_n]) = \dim(A) + n$

Proof. We can always assume that $n = 1$.

Case-1: Suppose $\dim(A) = \infty$. This implies $\dim(A[x]) < \infty$.

Case-2: Suppose $\dim(A) < \infty$. We prove by induction.

Case-2a: Suppose $\dim(A) = 0$, then it is either a field of a product of fields when modded out by the Nilpotent radical (does not change dimension). This implies $A[X]/\mathrm{Nil}(A)$ is a finite product of PIDs and hence we are done.

Case-2b: Assume $\dim(A) > 0$. Let $\mathfrak{p}$ be a prime ideal of A of height r. Let $q = \langle \mathfrak{p}[X], X \rangle$. Then, $q \in \mathrm{Spec}(A[X])$. Moreover $\mathrm{ht}(q) \geq \mathrm{ht}(\mathfrak{p}) + 1$. This implies $\dim(A[X]) \geq \dim(A) + 1$.

For the other direction, let $\dim(A) = n$ and $\mathfrak{m}$ be a maximal ideal of $A[X]$. Enough to show that $\mathrm{ht}(\mathfrak{m}) \leq n + 1$.
Take $\mathfrak{p} = \mathfrak{m} \cap A$. Recall that $\mathrm{ht}(\mathfrak{m}) = \mathrm{ht}(A_{\mathfrak{p}}[X]_{\mathfrak{m}})$. Hence, can assume that $(A, \mathfrak{p})$ is local. Now,
This implies there exists $f \in \mathfrak{m}$ such that $\mathfrak{m} = \langle f \rangle \Rightarrow \langle \mathfrak{p}[X], f \rangle = \mathfrak{m}$. Since, $\dim(A) = n$, we get that $\mathrm{ht}(\mathfrak{p}) \leq n$. Now, apply the previous proposition to observe that $\mathfrak{p}$ is a minimal prime of $\langle f_1, \ldots, f_r \rangle$ and thus $\mathfrak{m}$ is minimal prime of $\langle f_1, \ldots, f_r, f \rangle$ (needs to be checked). Finally, $\mathrm{ht}(\mathfrak{m}) \leq n + 1$. □

48.2. Geometric intuition of flatness

Suppose $\mathrm{Spec}(B) = X \xrightarrow{f} Y = \mathrm{Spec}(A)$ and f is flat.

Blabber (useful but blabber nonetheless)

Theorem 48.2.1.
Let $f : Y \to X$ be a flat morphism of affine schemes. Let $y \in Y$ and $x = f(y)$. Then,

$$\dim_x(Y_x) = \dim_y(Y) - \dim_x(X) \tag{48.3}$$

where $Y_x = \mathrm{Spec}(B \otimes_A k(x))$ if $X = \mathrm{Spec}(A)$ is the scheme theoretic fibre.

Proof. We can assume that A is local since the fibre remains the same whether we work with A or $A_{\mathfrak{p}}$.

If $\dim(A) = 0$, then it is a field and hence $\dim_x(X) = 0$ and $Y_x = \mathrm{Spec}(B \otimes_A k(x)) = \mathrm{Spec}(B)$ and hence we are done.

Assume $\dim(A) > 0$.

We can further assume that A is reduced and in a reduced ring, every associated prime is also minimal prime. □

49. Lecture-12 (15th February): Étale morphisms

Definition 49.0.1.
Let $f : Y \to X$ be a morphism of Noetherian affine schemes. If $y \in Y$ and $x = f(y)$. Then, f is said to be smooth at y if the following holds:

1. f is finite type at x
2. f is flat at y
3. $B_{\mathfrak{q}} \otimes_{A_{\mathfrak{p}}} \overline{k(x)}$ is regular

$X = \mathrm{Spec}(A), Y = \mathrm{Spec}(B), x = \mathfrak{p}, y = \mathfrak{q}$

We say that f is smooth if it is smooth at every point $y \in Y$

Part V.

Topics in Analytic Number Theory

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

51. Lecture-2:

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

Theorem 52.0.1 (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 $\lambda = \mathrm{Res}_{s=1} f(s) = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2)$

Lemma 52.0.2.
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 52.0.3.

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

Theorem 52.0.4 (Y. Zhang)**.**

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

Theorem 52.0.5.
If $\chi(q)$ does not have a Siegel zero, then $L(1,\chi) \gg \frac{1}{\log q}$

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

Lemma 53.0.1.
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 53.0.2.

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

Lemma 53.0.3.

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

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

Lemma 53.0.4.
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 53.0.5.
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 53.0.6.

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

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

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 53.0.7 (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 53.0.8 (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 53.0.9.
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

54. Tensor Products

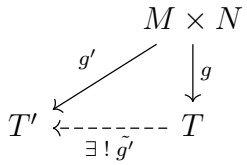
If M, N are abelian groups, what is $M \otimes_{\mathbb{Z}} N$. We will try to address this question. A bilinear map $\phi : M \times N \to P$ (P is an abelian group) is a function which is linear in both M, N. Tensor products are universal objects for all Bilinear maps from $M \times N$. In other words,

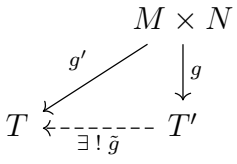
Theorem 54.0.1.
There exists pair $(T, g) \in \mathrm{Bilin}(M, N)$ satisfying the following properties:

1. Given any pair (P, ϕ) there exists an unique homomorphism $\tilde{\phi} : T \to P$ such that $\tilde{\phi} \circ g = \phi$.
2. If (T', g') is another pair which satisfies 1, then there exists an unique isomorphism $\theta : T \to T'$ such that $\phi \circ g = g'$.

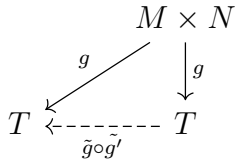
Proof.

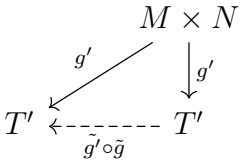
- **Uniqueness**: Suppose there are two pairs (T, g) and (T', g') satisfying 1. Then, we have two following two diagrams





Therefore





with $\tilde{g} \circ \tilde{g'} = \mathrm{id}_T$ and $\tilde{g'} \circ \tilde{g} = \mathrm{id}_{T'}$. This completes the first part. The uniqueness of isomorphism θ is also similar.

- **Existence**: Take C to the free abelian group on $M \times N$. Define $D \hookrightarrow C$ to be the subgroup generated by the relations:
  1. $(m + m', n) - (m, n) - (m', n)$
  2. $(m, n + n') - (m, n) - (m, n')$
  3. $(am, n) - a(m, n)$
  4. $(m, an) - a(m, n)$

  with $m, m' \in M, n, n' \in N, a \in \mathbb{Z}$
  Let $T := C/D$ and $g : M \times N \to T$ is defined by $g(m, n) = (m, n) \pmod{D}$.

The conditions imposed implies that g is bilinear. Next, suppose $(P, \phi) \in \mathbf{Bilin}(M, N)$, then we get a homomorphism $\tilde{\phi} : C \to P$ (by the universal property of free abelian groups).
$\because \phi$ is bilinear, $\tilde{\phi}$ kills all of D.
$\therefore$ it descends to a map $\tilde{\phi} : C/D \to P$ that is $phi : \tilde{T} \to P$
This completes the proof. □

Example 54.0.2.
$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$ since $1 \otimes 1 = 1 \otimes 4 = 2(1 \otimes 2) = 2 \otimes 2 = 0$

Exercise 54.0.3. *1. If $f : G \to H$ is a bijective group homomorphism, then f is an isomorphism.*

2. $\mathbb{Z}/mZZ \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(m, n)\mathbb{Z}$

3. If M, N are free abelian groups, then $M \otimes N$ is a free abelian group. Also, find the rank of $M \otimes N$ in terms of rank of M, N

4. M, N torsion implies $M \otimes N$ is torsion

Example 54.0.4.
Consider $M' = 2\mathbb{Z} \overset{\iota}{\hookrightarrow} M = \mathbb{Z}$ and $N = \mathbb{Z}/2\mathbb{Z}$. Take $\alpha = 2 \in M', \beta = 1 \in N$. Then,

$$M' \otimes N \xrightarrow{\iota \otimes \mathrm{id}_N} M \otimes N \tag{54.1}$$

says that $\alpha \otimes \beta = 0$ in $M \otimes N$. However, we claim that $\alpha \otimes \beta$ is nonzero in $M' \otimes N$. This is because ι is injective but the induced map $\iota \otimes \mathrm{id}_N$ is not injective. In other words, tensor products need not preserve monomorphisms but it must preserve epimorphisms.

Theorem 54.0.5.
Let M, N, P be abelian groups. Then there exists unique isomorphisms:

1. $M \otimes N \xrightarrow{\alpha} N \otimes M$
2. $(M \otimes N) \otimes P \xrightarrow{\beta} M \otimes (N \otimes P)$
3. $\mathbb{Z} \otimes M \xrightarrow{\gamma} M$
4. $(M \oplus N) \otimes P \xrightarrow{\delta} (M \otimes P) \oplus (N \otimes P)$

Proof. 1.

□

Definition 54.0.6.
An R-module is an abelian group M together with a group homomorphism

$$\phi_M : R \otimes M \longrightarrow M \tag{54.2}$$

such that

1. $$\begin{array}{ccc} R \otimes R \otimes M & \xrightarrow{\mathrm{id}_R \otimes \phi_M} & R \otimes M \\ \downarrow{\scriptstyle \mu_R \otimes \mathrm{id}_M} & & \downarrow{\scriptstyle \phi_M} \\ R \otimes M & \xrightarrow[\phi_M]{} & M \end{array}$$

2. $\phi_M(1 \otimes m) = m$ for all $m \in M$

Remark 54.0.7.
(1) gives us associativity, i.e.,

$$\begin{aligned} \phi : R \times M &\longrightarrow M \text{ bilinear with} \\ \phi(a, bm) &= (ab)m \; \forall \; m \in M, a, b \in R \end{aligned}$$

and (2) shows that $\phi(1, m) = m \; \forall \; m \in M$

Remark 54.0.8.
Abelian groups are just $\mathbb{Z}$-modules

Suppose M, N are R-modules. Then an R-linear map is just a group homomorphism $f : M \longrightarrow N$ such that $f(am) = af(m) \; \forall \; a \in R, m \in M$

Remark 54.0.9.

1. Every abelian group homomorphism is a $\mathbb{Z}$-linear map.
2. f is R-linear iff f commutes with the action of R on M.
3. R-linear maps are also called module homomorphisms.

A submodule of M is a subgroup M' of M such that the actions are preserved ($RM' = M'$)

If $f : M \to N$ is a module homomorphism, then $\ker(f)$ is a submodule of M and $\mathrm{Im}(f)$ is a submodule of N.

If $M \hookrightarrow N$, then N/M is an R-module homomorphism with the canonical projection $N \xrightarrow{\pi} N/M$ being R-linear.

Remark 54.0.10.
The category of R-modules is usually denoted by $\mathbf{Mod}_R$ or $R - \mathbf{mod}$

Suppose M, N are R-modules. Then, $\mathbf{Mod}_R$ has operations $\oplus$ and $\otimes_R$ such that

1. $M \otimes_R N \simeq N \otimes_R M$
2. $(M \oplus M') \otimes_R N \simeq (M \otimes_R N) \oplus (M' \otimes_R N)$
3. $R \otimes_R M \simeq M$

Remark 54.0.11.
Define $\mathrm{Hom}_R(M, N) = \{R\text{-linear maps from} M \to N\}$. It can be seen that $\mathrm{Hom}_R(M, N)$ is also a R-module such that

1. $(f + g)(m) = f(m) + g(m)$ for all $m \in M, f, g \in \mathrm{Hom}_R(M, N)$
2. $(af)(m) = af(m)$ for all $a \in R, m \in M, f \in \mathrm{Hom}_R(M, N)$

Definition 54.0.12.
Say M is a R-module. Then we define

$$M_{tor} = \{m \in M \mid am = 0 \text{ for some } 0 \neq a \in R\} \tag{54.3}$$

Exercise 54.0.13. *1. Prove or disprove that M_{tor} is a R-submodule.*

2. M is a torsion abelian group iff $M \otimes_{\mathbb{Z}} \mathbb{Q} = 0$

55. Ideals

An ideal I of R is a R-submodule of R such that $IR = I = RI$

Proposition 55.0.1.
Let I_1, I_2 be two ideals of R.

1. $I_1 \cap I_2$ is an ideal.
2. $I_1 \cup I_2$ might not be an ideal.
3. $I_1 I_2$ is an ideal.
4. $I_1 I_2 \subseteq I_1 \cap I_2$.

Exercise 55.0.2. *If I_1, I_2 are ideals such that $I_1 + I_2 = R$, then $I_1 \cap I_2 = I_1 I_2$*

Lemma 55.0.3.
For ideals I, J, K of R, we have $I(J + K) = IJ + IK$

For $I \subseteq R$ an ideal, we define the quotient ring R/I such that

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I)(b + I) = ab + I$
- $b(a + I) = ab + I$

Let $I_1, \dots, I_n \subseteq R$ be ideals and say we have a ring homomorphism

$$\begin{array}{ccc} R & \xrightarrow{Q} & \frac{R}{I_1} \times \cdots \times \frac{R}{I_n} \\ a & \longmapsto & (a + I_1, \dots, a + I_n) \end{array}$$

Exercise 55.0.4. *Show that* $\ker(Q) = \bigcap_{j=1}^{n} I_j$

Now,

$$\frac{R}{\ker Q} \xrightarrow{Q} \frac{R}{I_1} \times \cdots \times \frac{R}{I_n} \tag{55.1}$$

So, it is injective. We ask when is it surjective. Recall

Theorem 55.0.5 (Chinese Remainder Theorem)**.**
If $I_i + I_j = R$ for all $i \neq j$, then

1. $\displaystyle\bigcap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j$

2. $R/\prod_{j=1}^{n} I_j \simeq \prod_{j=1}^{n} R/I_j$

Definition 55.0.6. 1. $\mathfrak{p} \subseteq R$ is a prime ideal if $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$

2. $\mathfrak{m} \subseteq R$ is a maximal ideal if it is a proper ideal and for all proper ideals $\mathfrak{m}'$ such that $\mathfrak{m} \subsetneq \mathfrak{m}'$ implies $\mathfrak{m} = \mathfrak{m}'$

Proposition 55.0.7. 1. $\mathfrak{p}$ is a prime ideal iff $A/\mathfrak{p}$ is an integral domain.

2. $\mathfrak{m}$ is a maximal ideal iff $A/\mathfrak{m}$ is a field.

Theorem 55.0.8.
Every proper ideal is contained in a maximal ideal.

Definition 55.0.9. 1. $a \in R$ is called nilpotent if $a^n = 0$ for some $n \in \mathbb{Z}_{\geq 0}$

2. $\mathrm{Nil}(R) = \{a \in R : a \text{ is nilpotent } \}$

Theorem 55.0.10.

$$\mathrm{Nil}(R) = \bigcap_{\mathfrak{p}\text{: prime}} \mathfrak{p} \tag{55.2}$$

Definition 55.0.11.
Jacobson ideal of R = intersection of all maximal ideals.

In general, $\mathrm{Nil}(R) \subseteq \mathrm{Jac}(R)$

Exercise 55.0.12. *In* $R[X]$, $\mathrm{Jac}(R[X]) = \mathrm{Nil}(R[X])$

Theorem 55.0.13 (Theorem of prime avoidance)**.**
Let $I \subseteq R$ be an ideal and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be prime ideals such that $I \not\subseteq \mathfrak{p}_i \ \forall\ i$. Then, $I \not\subseteq \bigcup_{i=1}^{r} \mathfrak{p}_i$

Theorem 55.0.14.
If $I_1, \ldots, I_n \subseteq R$ are ideals such that $\bigcap_{j=1}^{n} I_j \subseteq \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal, then $I_i \subseteq \mathfrak{p}$ for some j.

Exercise 55.0.15. *Prove or disprove that a finite intersection of distinct prime ideals cannot be a prime ideal.*

Definition 55.0.16.
Let $I \subseteq R$ be an ideal. Then, the radical of I is defined as

$$\sqrt{I} = \{a \in R : a^n \in I \text{ for some } n \in \mathbb{Z}_{\geq 1}\} \tag{55.3}$$

Remark 55.0.17.
1. $I \subseteq \sqrt{I}$
2. If $I = \{0\}$, then $\sqrt{I}$ is the nilradical.
3. $R \xrightarrow{f} R/I$ implies $\sqrt{I} = f^{-1}(\mathrm{Nil}(R/I))$

Exercise 55.0.18.
1. *Suppose $\sqrt{I} + \sqrt{J} = R$. Then, $I + J = R$.*
2. *Show that $x \in \mathrm{Jac}(R) \Leftrightarrow 1 - xy \in R^\times \ \forall\ y \in R$*
3. *1,2,4,6,7,8,14 from chapter 1 Atiyah McDonald*

56. Modules

Theorem 56.0.1 (Cayley-Hamilton Theorem)**.**
Let $I \subseteq R$ be an ideal and M a f.g. R-module. Suppose ϕ is an endomorphism of M such that $\phi(M) \subseteq IM$. Then ϕ satisfies a polynomial equation

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0 \tag{56.1}$$

where $a_i \in I \; \forall \; i$

Corollary 56.0.2.
Let M be a f.g. R-module. Suppose $I \subseteq R$ is an ideal such that $IM = M$. Then there exists $a \in R$ such that $(1)a \equiv 1 \pmod{I}$ and $(2)aM = 0$.

Lemma 56.0.3 (Nakayama Lemma)**.**
Suppose M is a f.g. R-module. Suppose $I \subseteq \mathrm{Jac}(R)$ is an ideal such that $IM = M$, then $M = 0$.

Definition 56.0.4.
Let R be a commutative ring. R is called local if it has only one maximal ideal. We denote a local ring by $(R, \mathfrak{m}, k)$ where $\mathfrak{m}$ is the maximal ideal and k is the residue field.

Example 56.0.5.
fields, $\mathbb{Z}/n\mathbb{Z}$ where $n = p^f$

Example 56.0.6.
Fix a prime p. Set $\mathbb{Z}_{(p)} = \{\frac{m}{n} : p \nmid n\}$. Then, $\mathbb{Z}_{(p)}$ is a local ring with $p\mathbb{Z}_{(p)}$ as the only maximal ideal.

More generally, for an integral domain R and a prime ideal $\mathfrak{p}$ of R, $R_{\mathfrak{p}} = \{\frac{m}{n} : n \notin \mathfrak{p}\}$ is also a local ring

Remark 56.0.7.
Every element outside the maximal ideal is an unit in a local ring. The converse is also true.

Corollary 56.0.8.
Suppose R is a local ring with residue field k. If $M \otimes_R k = 0$, then $M = 0$.

Consider the categories

$$\begin{aligned} \mathbf{Mod}_R &\xrightarrow{\otimes_R k} k - \text{vector spaces} \\ M &\longmapsto M \otimes_R k \end{aligned}$$

Here, $M = 0 \Leftrightarrow M \otimes_R k = 0$ by the previous field. Hence, it is a conservative functor.

Definition 56.0.9.
Let

$$\mathcal{C} \xrightarrow{F} \mathcal{D} \tag{56.2}$$

We say F is conservative if $C = 0 \Leftrightarrow F(C) = 0$ where $C \in \mathrm{Ob}(\mathcal{C}), F(C) \in \mathrm{Ob}(\mathcal{D})$.

If V is a vector space over $\mathbb{F}$ and let V be a finite dimensional. Then,

$$\phi : V \twoheadrightarrow V$$

implies ϕ is an isomorphism. If we remove finite dimensionality, then this assertion is not true. For take $V = \mathbb{Z}[X]$ and ϕ be the polynomial derivative.

Theorem 56.0.10.
Let M be a R-module. If $\phi : M \twoheadrightarrow M$ is a surjection, then ϕ is an isomorphism.

Lemma 56.0.11 (Snake Lemma)**.**

Lemma 56.0.12.
Suppose we have a sequence

$$[*]M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{56.3}$$

Then, $*$ is exact iff the sequence

$$[*]0 \longrightarrow \mathrm{Hom}_R(M'', P) \xrightarrow{v^*} \mathrm{Hom}_R(M, P) \xrightarrow{u^*} \mathrm{Hom}_R(M', P) \tag{56.4}$$

is exact for all R-modules P.

Lemma 56.0.13.
Suppose we have a sequence

$$[*]M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{56.5}$$

Then, $*$ is exact iff the sequence

$$[*]0 \longrightarrow \mathrm{Hom}_R(P, M') \xrightarrow{v_*} \mathrm{Hom}_R(P, M) \xrightarrow{u_*} \mathrm{Hom}_R(P, M'') \tag{56.6}$$

is exact for all R-modules P.

Remark 56.0.14.
$\mathrm{Hom}_R(P, -)$ is a left exact functor. We claim that $\mathrm{Hom}_R(-, P)$ is not a right exact functor. Because consider

$$0 \longrightarrow M' \xrightarrow{u} M \tag{56.7}$$

Then

$$0 \longrightarrow \mathrm{Hom}_R(M, P) \xrightarrow{u^*} \mathrm{Hom}_{M',P} \tag{56.8}$$

need not be exact. For example,
take $R = \mathbb{Z}$

Theorem 56.0.15.
Suppose we have a sequence

$$[*]M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{56.9}$$

Then, $*$ is exact iff the sequence

$$[*]M' \otimes_R P \longrightarrow M \otimes_R P \longrightarrow M'' \otimes_R P \longrightarrow 0 \tag{56.10}$$

is exact for all R-modules P.

57. Projective, Injective, Flat modules

57.1. Flat and faithfully flat

Definition 57.1.1.
Let N be a R-module. Then, N is flat if $\otimes_R N : \mathbf{Mod}_R \to \mathbf{Mod}_R$ is exact.

Lemma 57.1.2.
TFAE:

1. N if flat
2. $M' \hookrightarrow M \Rightarrow M' \otimes N \hookrightarrow M \otimes N$
3. $M' \hookrightarrow M$ with M, M' f.g. implies $M' \otimes N \hookrightarrow M \otimes N$

Example 57.1.3. 1. every free module is flat.

2.

Exercise 57.1.4. *Let R be an integral domain with fraction field k. Then, k is R-flat.*

Definition 57.1.5.
F is called faithfully flat (ff) if for all sequences

$$[*]M' \longrightarrow M \longrightarrow M'' \tag{57.1}$$

$*$ is exact iff

$$[**]M' \otimes_R F \longrightarrow M \otimes_R F \longrightarrow M'' \otimes_R F \tag{57.2}$$

is exact.

Remark 57.1.6.
$ff \Rightarrow$ flat

Example 57.1.7.
Abelian $\Rightarrow ff$. Is the converse true? If $F = \mathbb{Q}$ ff as a $\mathbb{Z}$-module?

Notice that if M is finite abelian group, and

$$0 \to M \to 0$$

Then,

$$0 \to M \otimes \mathbb{Q} \to$$

which implies

$$0 \to 0 \to 0$$

Therefore $\mathbb{Q}$ is flat but not ff.

Theorem 57.1.8.
Let R be an integral domain with fraction field K. Suppose

$$R \hookrightarrow S \hookrightarrow K$$

are inclusions of rings. Then,

1. S is flat over R.
2. S is ff over R iff $S = R$.

Exercise 57.1.9. *Suppose F has the property that $M \otimes F = 0 \Leftrightarrow M = 0$. Is F ff?*

Theorem 57.1.10.
M is flat iff $I \otimes M \to M$ is injective for all ideal $I \subseteq R$.

Exercise 57.1.11.
1. *$R[X]$ is flat over R.*
2. *Direct sum(summand) is flat (if flat)*
3. *Tensor product of flat modules are flat.*
4. *Suppose R is an integral domain. Then, flat implies torsion-free.*
5. *Does torsion free implies flat?*

Theorem 57.1.12.
Let $R \to S \to T$ be a ring homomorphism. Then T is flat over S and S flat over R implies T is flat over R.

Exercise 57.1.13. *Let $R \to S$ be a ring homomorphism which is ff, $M \in \mathbf{Mod}_R$. Then, M is flat over R iff $M \otimes_R S$ is flat over S.*

Remark 57.1.14.
Let $R \to S$ be a ring homomorphism. Then, M is R-flat implies $M \otimes_R S$ is S-flat. Is the converse true?

Take $R = \mathbb{Z}, M = \mathbb{Z}/n\mathbb{Z}$. M is not flat over R since it is not torsion free but $M \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$

57.2. Projective Modules

Say F is a free R-module. Then we can ask two questions:

- Is the submodule free ?
- Is the direct summand free if F is free ?

Definition 57.2.1.
A R-module P is called projective if it is a direct summand of a free R-module.

Exercise 57.2.2. *1. Let $R = k[X, Y], M = R$. Take $I = \langle X, Y \rangle$. Show that I is not injective.*

2. Take $R = \mathbb{R}[X_1, X_2, X_3]/\langle X_1^2 + X_2^2 + X_3^2 - 1 \rangle$. Then,

$$0 \longrightarrow P \longrightarrow R^3 \longrightarrow R$$

$$\{e_1, e_2, e_3\} \qquad e_i \mapsto X_i$$

We see that $R^3 = R \oplus P$. Therefore, P is projective module by definition. But, it is an OPEN question whether P is free or not.

Theorem 57.2.3.
P is projective iff $\mathrm{Hom}_R(P, -)$ is an exact functor of $\mathbf{Mod}_R$ to $\mathbf{Mod}_R$

Remark 57.2.4.
Projective implies flat.

Theorem 57.2.5.
Suppose R is local, P a f.g. projective R-module. Then P is free.

57.3. Injective Modules

Definition 57.3.1.
We say that a R-module E is injective if $\mathrm{Hom}_R(-, E)$ is exact functor.

Example 57.3.2.
$\mathbb{Z}$ is not injective as $\mathbb{Z}$-module

Remark 57.3.3.
To show that E is injective, it suffices to show that

$$[*]0 \to M' \to M \tag{57.3}$$

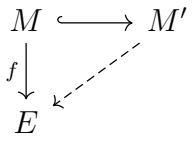
exact iff

$$[**]\mathrm{Hom}_R(M, E) \to \mathrm{Hom}_R(M', E) \to 0 \tag{57.4}$$

is exact.

i.e., $M' \hookrightarrow M \Rightarrow \mathrm{Hom}_R(M, E) \twoheadrightarrow \mathrm{Hom}_R(M', E)$

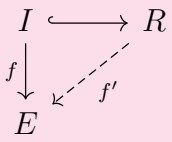
i.e., every map $f : M \to E$ extends



Exercise 57.3.4. *1. Show that $\mathbb{Q}$ is injective as $\mathbb{Z}$-module.*

2. Let M be a flat S-module and E an injective R-module. Then, $\mathrm{Hom}_R(M, E)$ is an injective S-module.

Theorem 57.3.5.
E is injective iff for all ideals $I \hookrightarrow R$ and homomorphism $f : I \to E$, there exists an extension $R \xrightarrow{f'} E$ of E, i.e.,



Definition 57.3.6.
We say that a R-module is divisible if $M \xrightarrow{\alpha} M$ is surjective for all $a \in R$, i.e., given $m \in R \exists\ n \in M$ such that $an = m$

Exercise 57.3.7. *1. Injective implies divisible.*

2. If R is PID, then injective iff divisible.

Remark 57.3.8.
$\mathbb{Q}$ is divisible implies $\mathbb{Q}/\mathbb{Z}$ is divisible. Also, $\mathbb{Z}$ is a PID therefore $\mathbb{Q}/\mathbb{Z}$ is injective.

Definition 57.3.9.
Let M be a R-module (thus it is also a $\mathbb{Z}$-module). Define

$$M^\vee := \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$$

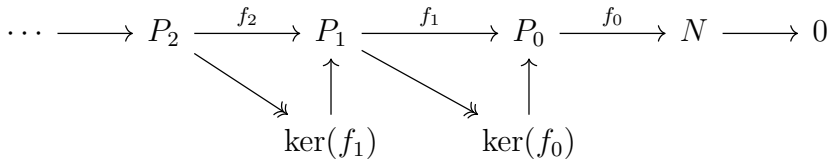
Remark 57.3.10.
If $M \neq 0$, then we can always construct a nonzero abelian group homomorphism $M \to \mathbb{Q}/\mathbb{Z}$. Thus, $M^\vee \neq 0$. For $M \in \mathbf{Mod}_R$ find $F \twoheadrightarrow M^\vee$. As F is free R-module therefore $M^\vee \hookrightarrow F^\vee$ as $\mathbb{Z}$-modules. Also, the evaluation map $M \hookrightarrow M^\vee$ is injective. Therefore $M \hookrightarrow F^\vee$

By a previous exercise, since F is flat (in fact free) R-module and $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, $\mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{Q}/\mathbb{Z}) = F^\vee$ is injective R-module. Thus, $M \hookrightarrow F^\vee$, i.e., M sits inside an injective module.

Remark 57.3.11.
In the category of R-modules, every module sits inside an injective module.

57.4. Applications

Suppose M, N are R-modules. We know that N is a quotient of projective (in fact free) module. Thus, we can construct an exact sequence as follows:



This is called a projective resolution of N. We write it as $P \to N \to 0$.

Then, $P \otimes_R M \to N \otimes_R M \to 0$ is a chain complex (not necessarily exact). We define

$$\mathrm{Tor}_R^i(M, N) := H_i(P \otimes_R N), i \geq 0$$

Also, it can be proven that

$$\mathrm{Tor}_R^i(M,N) = \mathrm{Tor}_R^i(N,M), \text{ and} \tag{57.5}$$
$$\mathrm{Tor}_R^0(M,N) = M \otimes_R N \tag{57.6}$$

Theorem 57.4.1.
Let M be a R-module. TFAE:

1. M is flat
2. $\mathrm{Tor}_R^i(M,N) = 0 \; \forall \; i > 0, \forall \; N$
3. $\mathrm{Tor}_R^1(M,N) = 0 \; \forall \; N$

Exercise 57.4.2. *For $I \subseteq R$ an ideal, M a R-module, we have*

$$\mathrm{Tor}_R^1(R/I, M) = \{m \in M : am = 0 \; \forall \; a \in I\}$$

Exercise 57.4.3. *1,3,4,5,7,8,10,11 from Atiyah McDonald chapter 2*

58. Noetherian and Artinian Rings

Let Σ be a poset with the order given by $\leq$

Proposition 58.0.1.
TFAE:

1. Every increasing chain $x_1 \leq x_2 \leq \cdots$ is stationary.
2. Every non-empty subset of Σ has a maximal element.

Definition 58.0.2.
Suppose Σ is a set whose subsets are ordered by inclusions. If Σ satisfies any of the conditions of the previous proposition, we say that the subsets of Σ satisfy the ascending chain condition (acc). If the subsets of Σ are ordered by $\geq$ then we say that the subsets of Σ satisfy the descending chain condition (dcc).

Definition 58.0.3.
1. We say that the R-module M is Noetherian if its submodules satisfy acc.
2. We say that the R-module M is Artinian if its submodules satisfy dcc.

Example 58.0.4.
1. M a finite abelian group is both Noetherian and Artinian.
2. $\mathbb{Z}$ as a $\mathbb{Z}$-module is Noetherian ($\mathbb{Z}$ is a Noetherian ring) since every element can be factored into finitely many irreducibles. But $\mathbb{Z}$ is not Artinian since
$$\mathbb{Z}/2\mathbb{Z} \supseteq \mathbb{Z}/4\mathbb{Z} \supseteq \mathbb{Z}/8\mathbb{Z} \supseteq \cdots$$
3. Let k be a field. Then a k-module M is just a k-vector space. Therefore M is Noetherian as k-module iff M is finite dimensional iff M is Artinian as a k-module. In particular, k itself is just 1-dimensional k-module. Therefore k is Noetherian ring.
4. Let $R = \mathbb{Z}, p$ a prime. $M = \{x \in \mathbb{Q}/\mathbb{Z} \mid p^m x = 0 \text{ for some } m \geq 0\}$. Then M is a Noetherian R-module. This follows from the following claim:
Claim: The only subgroups of M are of the form $(\frac{1}{p^m}\mathbb{Z})/\mathbb{Z} \simeq \mathbb{Z}/p^m\mathbb{Z}$

   Proof. □

In fact, look at

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \hookrightarrow \mathbb{Z}/p^3\mathbb{Z} \hookrightarrow \cdots$$

$$1 \longmapsto p \longmapsto p^2$$

Then $M = \varinjlim \mathbb{Z}/p^n\mathbb{Z}$. It can be shown that M is Artinian but not Noetherian.

5. Let $M = \{m/p^n \mid n \geq 0, m \in \mathbb{Z}\} \hookrightarrow \mathbb{Q}$. Then,

$$M \hookrightarrow \mathbb{Q} \twoheadrightarrow \mathbb{Q}/\mathbb{Z}, \quad \alpha : M \to \mathbb{Q}/\mathbb{Z}$$

$N = \ker(\alpha), N'\mathrm{Im}(\alpha)$. Then

$$0 \to N \to M \to N' \to 0$$

is exact. But M is neither Noetherian nor Artininan.

Remark 58.0.5.
View R as a R-module over itself. If the module is Noetherian then it has to be Artinian.

Proposition 58.0.6.
M is Noetherian iff every submodule of M is f.g.

Example 58.0.7.
Let $R = k[X_1, \ldots, X_i, \ldots]$. We know that R is not Noetherian since

$$k \subseteq k[X_1] \subseteq k[X_1, X_2] \subseteq \cdots$$

But $R \hookrightarrow \mathrm{Frac}(R)$ and $\mathrm{Frac}(R)$ is Noetherian.
Next, $R \subseteq S = \{a/b : X_1 \nmid b\} \subseteq F$. Is S Noetherian?

Theorem 58.0.8.
R is Noetherain iff every prime ideal of R is f.g.

Proposition 58.0.9.
Let

$$(*)0 \to M' \to M \to M'' \to 0$$

be exact sequence of R-modules. Then

1. M is Noetherian iff M' and M'' are.

2. M is Artinian iff M' and M'' are.

Corollary 58.0.10.
If $M = \bigoplus_{i=1}^{n} M_i$, then M is Noetherian (Artinian) iff M_i's are Noetherian (Artinian).

Definition 58.0.11.
We say that R is Noetherian (resp. Artinian) if it is Noetherian (resp. Artinian) as a R-module.

Example 58.0.12.
Let X be an infinite compact Hausdorff space and $\mathsf{C}(X)$ the set of continuous functions from X to $\mathbb{R}$. Then, is (X) a Noetherian ring?

Exercise 58.0.13. *A compact Hausdorff space is Noetherian iff it is infinite.*

Proposition 58.0.14.
Suppose $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are maximal ideals of R such that $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Then, R is Noetherian iff R is Artinian.

Corollary 58.0.15.
Suppose $(R, \mathfrak{m})$ is a Noetherian local ring such that $\mathfrak{m}^n = 0$. Then, R is Artinian.

Remark 58.0.16.
In previous proposition, we use the fact that $\mathfrak{m}_i$ are the only maximal ideals. For, take $\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Then $2\mathbb{Z}$ is a maximal ideal such that $(2\mathbb{Z})^2 = 0$ but it is not Artinian.

Exercise 58.0.17. *1,2,4,5,6,7,8 of Atiyah McDonald chapter 6*

Lemma 58.0.18.
Suppose R is Noetherian and S is a R-algebra such that S is f.g. as a R-module. Then, S is also a Noetherian ring.

Theorem 58.0.19 (Hilbert Basis Theorem)**.**
Let R be a Noetherian Ring. Then $R[X]$ is also Noetherian.

Proof. □

Corollary 58.0.20.
R is Noetherian iff $R[X_1, \ldots, X_n]$ is Noetherian.

Definition 58.0.21.
If S is a R-algebra, then we say that S is of finite type (f.g.) over R if $exists\ x_1, \ldots, x_n \in S$ such that every element of S is a polynomial in $\{x_1, \ldots, x_n\}$ with coefficients in R.

This is equivalent to saying there is a surjection of R-algebra $R[x_1, \ldots x_n] \twoheadrightarrow S$

Corollary 58.0.22.
R is Noetherian and S a f.g. R-algebra implies S is Noetherian.

58.1. Power Series Ring over R

Denote by $R[[X]] = \{\sum_{i\geq 0} a_i X^i \mid\ a_i \in R\}$

Clearly, $R \hookrightarrow R[X] \hookrightarrow R[[X]]$

Theorem 58.1.1.
If R is Noetherian, then $R[[X]]$ is Noetherian.

58.1.1. Interlude to complex analysis

Let R be the ring of all holomorphic functions on $\mathbb{C}$ which are holomorphic on some neighbourhood of 0.

Also, $I = \{f \in R : f(0) = 0\}$ is the only maximal ideal of R. Thus, R is a local ring. Is R Noetherian?

Observe that $R = \mathbb{C}\{X\} \hookrightarrow \mathbb{C}[[X]]$ where $\mathbb{C}\{X\}$ the ring of convergent power series. Thus,

$$\mathbb{C} \hookrightarrow \mathbb{C}[X] \hookrightarrow \mathbb{C}\{X\} = R \hookrightarrow \mathbb{C}[[X]]$$

We know that all the terms in the sequence except R are Noetherian, so we guess that R is also Noetherian. This is, in fact, true.

Proposition 58.1.2.
Let S be a R-algebra which is faithfully flat. Suppose that S is Noetherian. Then, R is also Noetherian.

Using this proposition and the fact that

$$\mathbb{C}\{X\} \hookrightarrow \mathbb{C}[[X]]$$

is a ff extension, we deduce that $\mathbb{C}\{X\}$ is Noetherian.

Corollary 58.1.3.
Let $(R, \mathfrak{m}) \hookrightarrow (S, \mathfrak{m}')$ be a local ring homomorphism that is also flat. Then, S Noetherian implies R Noetherian.

Using this corollary. and the fact that

$$\mathbb{C}\{X\} \hookrightarrow \mathbb{C}[[X]]$$

is a local ring homomorphism, it suffices to check that this extension is flat to deduce that $\mathbb{C}\{X\}$ is Noetherian.

Definition 58.1.4.
A R-module M is said to be faithful if $aM \neq 0 \; \forall \; 0 \neq a \in R$, .i.e., the annihilator of M is $\{0\}$.

Proposition 58.1.5.
Let M be a R-module. If M is Noetherian and faithful, then R is a Noetherian ring.

Theorem 58.1.6 (Eakin-Nagata)**.**
Let $R \subseteq S$ be an inclusion of rings such that S is Noetherian ring and is f.g. R-module. Then, R is a Noetherian ring.

Let M be a R-module. Then,

$$R \text{ Noetherian} \Leftrightarrow I \subseteq R \text{ is f.g.} \;\Leftrightarrow \mathfrak{p} \subseteq R \text{ is f.g.}$$

- Suppose IM is f.g. for all $I \subsetneq R$. Is M Noetherian?
- Suppose $\mathfrak{p}M$ is f.g. for all $\mathfrak{p} \subsetneq R$. Is M Noetherian?

Turns out that both are false! Take $R = k$ a field and M an infinite dimensional vector space. This gives us a counterexample. What happens if M is f.g.

Theorem 58.1.7.
Suppose M is a f.g. R-module. Then,

$$M \text{ Noetherian} \;\Leftrightarrow IM \text{ is f.g.} \forall \; I \subsetneq R \Leftrightarrow \mathfrak{p}M \text{ is f.g. } \forall \; \mathfrak{p} \subseteq R$$

Proposition 58.1.8.
Let $(R, \mathfrak{m}, k)$ be a local Noetherian ring. If M is a f.g. R-module. Then TFAE:

1. M is free.
2. M is flat.
3. $\mathfrak{m} \otimes M \to M$ is injective.
4. $\operatorname{Tor}_R^1(k, M) = 0$

59. Nullstellansatz

59.1. Interlude to algebraic geometry

Let R be a commutative ring, $X = \operatorname{Spec}(R) =$ the set of all prime ideals of R. Declare a subset of X to be closed if it is of the form

$$\mathcal{V}(I) = \{\mathfrak{p} \mid I \subseteq \mathfrak{p}\}$$

where I is a fixed ideal of R.

Exercise 59.1.1. *Show that this defines a topology on X. This topology is called the Zariski topology.*

Definition 59.1.2.
An affine scheme is a commutative ring R together with the Zariski topology of $\operatorname{Spec}(R)$.

Exercise 59.1.3. 1. *$\forall\ f \in R$, define $X_f = \{\mathfrak{p} \mid f \notin \mathfrak{p}\} \subseteq X$. Then, show that each X_f is open in the Zariski topology. Also, prove that $\{X_f\}$ is a basis for the Zariski topology on $\operatorname{Spec}(R)$.*

2. *Show that $\operatorname{Spec}(R)$ is quasi-compact.*

Definition 59.1.4.
A topological space is called irreducible if the intersection of any two non-empty open sets is non-empty. This can be extended to say that that intersection of finitely many non-empty open sets is non-empty.
Equivalently, X is not a finite union of closed sets unless one of the closed sets is all of X.

Remark 59.1.5.
X cannot be irreducible by definition if it is Hausdorff.

Exercise 59.1.6. *Suppose R is an integral domain. Show that $\operatorname{Spec}(R)$ is irreducible.*

Example 59.1.7. 1. Let $R = \mathbb{C}[t], X = \operatorname{Spec}(R)$. We wish to compare the Zariski topology on X and the natural Euclidean topology on $\mathbb{C}$. To make this more concrete, observe that the only prime ideals of $\mathbb{C}[t]$ are of the form $\langle f \rangle$ where f is an irreducible polynomial. But, the only irreducibles are the linear and

constant polynomials. Now,

$$\Phi : \langle f \rangle \longrightarrow \text{ zeroes of } f$$

is actually surjective from $X \backslash \{0\}$ to $\mathbb{C}$.

2. Let $R = \mathbb{R}[t], X = \mathrm{Spec}(R)$

Remark 59.1.8.
1. If $f \xrightarrow{f} S$ is a ring homomorphism, then $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ given by $\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})$ is a continuous map.
2. For $R \xrightarrow{\pi} R/I$ we have $\pi^* : \mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ is bijective and closed immersion.
3. For $R \xrightarrow{\pi} R/\mathrm{Nil}(R)$ we have $\pi^* : \mathrm{Spec}(R/\mathrm{Nil}(R)) \to \mathrm{Spec}(R)$ is a homeomorphism. In other words, Zariski topology does not see the nilradical. More precisely, while studying $\mathrm{Spec}(R)$ we can just work with $\mathrm{Spec}(R/\mathrm{Nil}(R))$ and assume R is reduced ring (has no nonzero nilpotent elements).

Fix a field k, let $R = k[X_1, \ldots, X_n], X = \mathrm{Spec}(R), X_{Zar} = \mathrm{maxsp}(R) =$ all maximal ideals , $X_{an} = k^n$
Define

$$\begin{aligned} \phi : X_{an} &\longrightarrow X_{Zar} \\ (a_1, \ldots, a_n) &\mapsto \langle X_1 - a_1, \ldots, X_n - a_n \rangle \end{aligned}$$

If k has its own topology, then X_{an} gets the product topology. In this case, is ϕ continuous ?

Any closed set in X_{Zar} is of the form

$$\mathcal{V}(I) = \{\text{maximal ideals containing } I\}$$

for some ideal $I \subseteq R$.

Then, $\phi^{-1}(\mathcal{V}(I)) = \{(a_1, \ldots, a_n) : \mathcal{V}(X_1 - a_1, \ldots, X_n - a_n) \subseteq \mathcal{V}(I)\}$. But since R is Noetherian we must have $I = \langle f_1, \ldots, f_r \rangle$.

Thus,

$$\phi^{-1}(\mathcal{V}(I)) = \{(a_1, \ldots, a_n) : f_i(a_1, \ldots, a_n) = 0 \; \forall \; 1 \leq i \leq r\}$$

In this case $k = \mathbb{R}$, clearly $\phi^{-1}(\mathcal{V}(I))$ is closed as it is the intersection of set of zeroes of polynomials. Therefore ϕ is continuous when $k = \mathbb{R}$ or $\mathbb{C}$. Moreover, ϕ is bijective as well.

However, ϕ is not a closed map. Take $k = \mathbb{R}$ or $\mathbb{C}$ and $Z = \{z : \sin z = 0\}$. Then, Z is infinite and thus it is not closed in the Zariski topology. However, it is closed in the Euclidean topology. Thus, Z is analytically closed but not Zariski closed.

Definition 59.1.9.
A subset $Z \subseteq k^n$ is said to be algebraic if there exists a set $S \subseteq R$ such that $Z = \{(a_1, \ldots, a_n) : f(a_1, \ldots, a_n) = 0 \; \forall \; f \in S\}$

For $Z \subseteq k^n$, $\mathcal{I}(Z) = \{f \in R : f(a_1, \ldots, a_n) = 0 \; \forall \; (a_1, \ldots, a_n) \in Z\}$ is an ideal in R

For an ideal $I \subseteq R$, we define

$$\mathcal{V} = \{(a_1, \ldots, a_n) : f(a_1, \ldots, a_n) = 0 \; \forall \; f \in I\}$$

Observe that $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$

Let $\Sigma_{Zar} =$ set of all radical ideals of R and $\Sigma_{an} =$ the set of all algebraic subsets of k^n

We define $\Phi : \Sigma_{Zar} \longrightarrow \Sigma_{an}$ by $I \mapsto \mathcal{V}(I)$

Clearly, Φ is a surjection. We would like to show that this is also an injection. But this need not be true in general.

Example 59.1.10.
$k = \mathbb{R}, I_1 = \langle X^2 + 1 \rangle, I_2 = \langle X^2 + 2 \rangle$. Then, $\Phi(I_1) = \Phi(I_2) = \emptyset$ therefore Φ need not be injective here. Thus, we need an additional assumption. Hence, we assume that k is algebraically closed.

59.2. Hilbert Nullstellansatz

Theorem 59.2.1 (Hilbert Nullstellansatz)**.**
Let k be an algebraically closed field, then Φ is bijective. In fact, for every ideal $I \subseteq R, \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. Thus, for radical ideals $I_1, I_2, \mathcal{V}(I_1) = \mathcal{V}(I_2) \Rightarrow \mathcal{I}(\mathcal{V}(I_1)) = \mathcal{I}(\mathcal{V}(I_2)) \Rightarrow \sqrt{I_1} = \sqrt{I_2} \Rightarrow I_1 = I_2$

Lemma 59.2.2.
Let A be a Noetherian ring. Let $B \hookrightarrow C$ be an inclusion of A-algebras such that C is f.g. as A-algebra over A and f.g. as a B-module over B. Then, B is f.g. over A. In particular, B is Noetherian.

Lemma 59.2.3.
Let k be a field and E a f.g. k-algebra. Suppose that E is a field. Then E is a finite field extension of k.

Lemma 59.2.4.
Let k be a field, $E = k[X]/\langle X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0\rangle$. Then, E is f.g. k-module.

Corollary 59.2.5.
Let k be a field, A a f.g. k-algebra, $\mathfrak{m} \hookrightarrow A$ maximal ideal. Then, $A/\mathfrak{m}$ is a finite algebraic extension of k. In particular, $k \cong A/\mathfrak{m}$ if k is algebraically closed.

Proof of Nullstellansatz. □

If $k = \bar{k}$, then $\phi : X_{an} \to X_{Zar}$ defined before is a bijection.

Consider the maximal ideal $\mathfrak{m} \hookrightarrow R = k[X_1, \ldots, X_n]$. Then,

$$k \hookrightarrow R \xrightarrow{\phi} k = R/\mathfrak{m}$$

And, $I = \langle X_1 - a_1, \ldots, X_n - a_n\rangle$ is maximal. $\phi(I) = 0 \Rightarrow I \subseteq \ker\phi = \mathfrak{m} \Rightarrow \langle X_1, \ldots, X_n\rangle = \mathfrak{m}$.

Corollary 59.2.6.
Suppose $k = \bar{k}$. Suppose we have a system of polynomial equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_n(x_1, \ldots, x_n) &= 0 \end{aligned}$$

Then this system has no solution in k^n iff there exists polynomials $g_1, \ldots, g_r$ such that $\sum_{i=1}^{m} f_i g_i = 1$

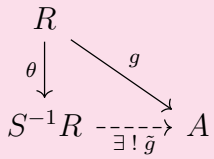
Exercise 59.2.7. *1,6,10,13 from Atiyah McDonald chapter 7*

60. Localisation

Let R be a commutative ring, S a multiplicatively closed subset containing 1.

Theorem 60.0.1.
There exists a ring homomorphism $\theta : R \to S^{-1}R$ which has the following properties:

1. $\theta(s) \in (S^{-1}R)^\times \ \forall\ s \in S$
2. Given any ring homomorphism $g : R \to A$ such that $g(s) \in A^\times \ \forall\ s \in S$ $\exists\,!$ ring homomorphism $\tilde{g} : S^{-1}R \to A$ such that $g = \tilde{g} \circ \theta$.



Proof. Existence: Define the relation on $R \times S$ given by $(a, s) \sim (a', s')$ if $t(as' - a's) = 0$ for some $t \in S$. It can be checked that this is an equivalence relation. Define □

Remark 60.0.2.
$\ker \theta = \{a \in R : as = 0 \text{ for some } s \in S\}$. This is because $\theta(a) = 0 \Leftrightarrow \frac{a}{1} = \frac{0}{1}$ in $S^{-1}R \Leftrightarrow (a, 1) \sim (0, 1) \Leftrightarrow (a \cdot 1 - 0 \cdot 1)s = 0$ for some $s \in S$

In particular, if R is an integral domain, then $\theta : R \to S^{-1}R$ is injective.

Let M be a R-module. We can define

$$S^{-1}M = (M \times S)/\sim$$

where $(m, s) \sim (m', s')$ if $(ms' - m's)t = 0$ for some $t \in S$. We denote by $[(m, s)]$ by $\frac{m}{s}$. By definition, it is clear that

1. $S^{-1}M$ is a $S^{-1}R$ module by the action
$$\frac{a}{s} \cdot \frac{m}{s'} = \frac{am}{ss'}$$
2. $\theta_M : M \to S^{-1}M$ given by $m \mapsto m/1$ is a R-module homomorphism

Proposition 60.0.3.
The functor $\mathbf{Mod}_R \to \mathbf{Mod}_{S^{-1}R}$ given by $M \mapsto S^{-1}M$ is an exact functor.

Consider

$$\begin{aligned} \alpha : S^{-1}M \times M &\to S^{-1}M \\ (\frac{a}{s}, m) &\mapsto \frac{am}{s} \end{aligned}$$

We can check that α is a bilinear R-module homomorphism. Hence, α induces a R-linear map

$$\begin{aligned} \alpha : S^{-1}M \otimes_R M &\to S^{-1}M \\ \frac{a}{s} \otimes m &\mapsto \frac{am}{s} \end{aligned}$$

It is easy to see that α is in fact $S^{-1}R$ linear since

$$\begin{aligned} \alpha\left(\frac{a'}{s'}\left(\frac{a}{s} \otimes m\right)\right) &= \alpha\left(\frac{aa'}{ss'} \otimes m\right) \\ &= \frac{aa'm}{ss'} \\ &= \frac{a'}{s'}\alpha\left(\frac{a}{s} \otimes m\right) \end{aligned}$$

Theorem 60.0.4.
α is an isomorphism.

Corollary 60.0.5.
$S^{-1}R$ is flat over R.

Remark 60.0.6.
However, if $S \backslash R^\times \neq \emptyset$ then $S^{-1}R$ is not ff. Take $a \in S$ such that $a \notin R^\times$. Then, $\langle a \rangle \neq R$ so if $I = \langle a \rangle$ then R/IR is a nonzero R-module. Any element of R/IR is of the form $r + I$.

In $R/IR \otimes_R S^{-1}R$

$$\begin{aligned} (r+I) \otimes \frac{b}{t} &= (ar+I) \otimes \frac{b}{at} \\ &= I \otimes \frac{b}{at} \\ &= 0 \end{aligned}$$

Hence, $R/IR \otimes_R S^{-1}R = \{0\}$. Thus,

$$0 \longrightarrow R/IR \longrightarrow 0$$

is not exact but

$$0 \longrightarrow R/IR \otimes_R S^{-1}R \longrightarrow 0$$

is exact. Hence, $S^{-1}R$ is almost never ff.

Example 60.0.7.

1. Let R be a ring and $\mathfrak{p}$ be a prime ideal. Let $S = R\backslash\mathfrak{p}$. Then, S is multiplicatively closed. We write $R_\mathfrak{p} := S^{-1}R$

   Claim: $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$

2. Let $f \in R\backslash\{0\}$. Set $S = \{f^n \mid n \geq 0\}$. Then, S is a multiplicatively closed and so we can write $R_f := S^{-1}R$.

   Observe that $R_\mathfrak{p} = \varinjlim_{f \in \mathfrak{p}} R_f$.

3. If $R = \mathbb{Z}, S = \mathbb{Z}\backslash\langle p\rangle$ for some prime p, then

   $$S^{-1}R = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$$

4. Let k be a field, $R = k[X_1, \ldots, X_n]$. Suppose $k = \bar{k}$. Then by Nullstellansatz, every maximal ideal of R is of the form $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n\rangle$ for some $(a_1, \ldots, a_n) \in k^n$.
   We also had the continuous map $\theta : \mathbb{C}^n \to \mathbb{C}^n_{Zar}$. Then, for $\mathfrak{m}\langle X_1 - a_1, \ldots, X_n - a_n\rangle$, we have $R_\mathfrak{m} = \mathcal{O}_{X,x}$ the ring of rational functions which are regular (holomorphic) in a Zariski neighbourhood of $x = (a_1, a_2, \ldots, a_n)$. This is because any element of $R_\mathfrak{m}$ is a rational function f/g with $g \notin \mathfrak{m}$, i.e., g does not vanish at x. Hence, if $A = \{y \in X \mid g(y) = 0\}$, then A is Zariski closed. Thus, A^c is Zariski neighbourhood of x. Hence, g is nonvanishing on a Zariski neighbourhood of x. Thus, f/g is regular in this Zariski neighbourhood of x.

   Since the topology is finer than the Zariski topology, we get the inclusion of local rings

   $$\mathcal{O}_{X_{Zar},x} \hookrightarrow \mathcal{O}_{X_{an},x}$$

   ring of rational functions which are regular in a Zariski nbd of $x$ring of rational functions which

Proposition 60.0.8.
Localisation commutes with tensor product, i.e., if M, N are R-modules, $S \subseteq R$

multiplicatively closed set, then

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_R N)$$
$$\frac{m}{s} \otimes \frac{n}{s'} \mapsto \frac{m \otimes n}{ss'}$$

Remark 60.0.9.
Also, $S^{-1}(M \oplus N) \simeq S^{-1}M \oplus S^{-1}N$ as $S^{-1}R$ modules by the mapping $\frac{m+n}{s} \mapsto \frac{m}{s} + \frac{n}{s}$. Notice that

$$S^{-1}M \oplus S^{-1}N \simeq (S^{-1}R \otimes_R M) \oplus (S^{-1}R \otimes_R N) \simeq S^{-1}R \otimes_R (M \oplus N) \simeq S^{-1}(M \oplus N) \tag{60.1}$$

What are the ideals of $S^{-1}R$ and how do they relate to ideals of R?
We have

$$\theta : R \to S^{-1}R \tag{60.2}$$

For ideal $I \subseteq R$, $T^e = \theta(I)S^{-1}R$ is an ideal of $S^{-1}R$.
For ideal $J \subseteq S^{-1}R$, $J^c = \theta^{-1}(J)$ is an ideal of R.

Lemma 60.0.10.
For ideal $I \subseteq R$, $I^e = S^{-1}I$

Lemma 60.0.11.
Every ideal of $S^{-1}R$ is an extended ideal, i.e., of the form I^e for some ideal $I \subseteq R$

Lemma 60.0.12.
Let $I \subseteq R$ be an ideal. Then we know that $I^e \hookrightarrow S^{-1}R$ is an ideal, and $I \hookrightarrow I^{ec}$.
In fact,

$$I^{ec} = \bigcup_{s \in S} (I : s)$$

where $(I : s) = \{a \in R \mid as \in I\} \supseteq I$

Corollary 60.0.13.
If $\mathfrak{p} \subseteq R$ is a prime ideal, then $\mathfrak{p} = \mathfrak{p}^{ec}$ (if $\mathfrak{p} \cap S = \emptyset$)

Corollary 60.0.14.
Every proper ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal $I \subseteq R$ such that $I \cap S = \emptyset$

Exercise 60.0.15. *An ideal of R is a contracted ideal iff no element of S is a zero divisor of R/I*

60.1. Prime ideals in $S^{-1}R$

Proposition 60.1.1.

$$\{\text{prime ideals of } R \text{ disjoint from } S\} \to \{\text{all prime ideals of } S^{-1}R\}$$
$$\mathfrak{p} \longmapsto S^{-1}\mathfrak{p}$$

This correspondence is well-defined and a bijection. Thus, $\mathrm{Spec}(S^{-1}R) \hookrightarrow \mathrm{Spec}(R)$ is an inclusion of spaces.

Exercise 60.1.2. *Let $I \subseteq R$ be an ideal. Then,*

$$S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$$

Corollary 60.1.3.

$$\mathrm{Nil}(S^{-1}R) = S^{-1}\mathrm{Nil}(R) \tag{60.3}$$

Proposition 60.1.4.
Let $\mathfrak{p} \subseteq R$ be a prime ideal. Then,

$$\mathrm{Spec}(R_{\mathfrak{p}}) = \bigcap_{f \notin \mathfrak{p}} \mathrm{Spec}(R_f) \tag{60.4}$$

Let P be a property of modules (or rings) over commutative rings. Then, we say that P is local if for every R-module M

$$M \text{ has } P \text{ as a } R \text{ module } \Leftrightarrow M_{\mathfrak{p}} \text{ has } P \text{as a } R_{\mathfrak{p}} \text{ module } \forall\, \mathfrak{p} \subseteq R \tag{60.5}$$

Proposition 60.1.5.
Let M be a R-module. TFAE:

1. $M = 0$
2. $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$
3. $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m} \in \mathrm{maxSpec}(R)$

Proposition 60.1.6.
Let $\phi : M \to N$ be a R-linear map. TFAE:

1. ϕ is injective
2. $\phi_{\mathfrak{p}}$ is injective for all $\mathfrak{p} \in \mathrm{Spec}(R)$

3. $\phi_{\mathfrak{m}}$ is injective for all $\mathfrak{m} \in \mathrm{maxSpec}(R)$

Proposition 60.1.7.
Let M be a R-module. TFAE:

1. M is R-flat
2. $M_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$-flat for all $\mathfrak{p} \in \mathrm{Spec}(R)$
3. $M_{\mathfrak{m}}$ is $R_{\mathfrak{m}}$-flat for all $\mathfrak{m} \in \mathrm{maxSpec}(R)$

Exercise 60.1.8. *2,3,4,5,6,8,13,17 from Atiyah McDonald chapter 3*

61. Integral extensions

Proposition 61.0.1.
Let $A \subseteq B \subseteq C$ be inclusions of commutative rings. If B is integral over A and C is integral over B, then C is integral over A

Corollary 61.0.2.
Let $A \subseteq B$ be an inclusion of rings. Let C be the integral closure of A in B. Then, C is integrally closed in B.

Proposition 61.0.3.
Suppose $A \subseteq B$ is an integral extension.

1. Let $J \subseteq B$ be an ideal and let $I = J \cap A = J^c$. Then, $A\mathcal{I} \subseteq B/J$ is an integral extension.
2. If $S \subseteq A$ is a multiplicatively closed set, then $S^{-1}A \subseteq S^{-1}B$ is an integral extension.

Theorem 61.0.4.
Let $f : B \to B'$ be an integral extension of A-algebras and let C be an A-algebra. Then, $f \otimes_A 1 : B \otimes_A C \to B' \otimes_A C$ is an integral extension.

Proposition 61.0.5.
Let $A \subseteq B$ be an inclusion of integral domains. Assume that B is integral over A. Then, A is a field iff B is a field.

Corollary 61.0.6.
$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not an integral domain

Corollary 61.0.7.
Let $A \subseteq B$ be an integral extension of rings. Let $\mathfrak{q} \subseteq B$ be a prime ideal. We already know that $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$ is a prime ideal of A. Then, $\mathfrak{q}$ is maximal in B iff $\mathfrak{p}$ is maximal in A.

Remark 61.0.8.
In general, neither implication is true. Consider $\mathbb{Z} \hookrightarrow \mathbb{Q}$ and $\mathbb{Q} \to \mathbb{Q}[X]$ for counterexamples.

Corollary 61.0.9.
Let $A \subseteq B$ be an integral extension of rings. Let $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq B$ be two prime ideals. Then, $\mathfrak{q}_1 = \mathfrak{q}_2$ iff $\mathfrak{q}_1^c = \mathfrak{q}_2^c$

Theorem 61.0.10.
Let $A \subseteq B$ be an integral extension. Let $f : A \to B$ be this inclusion. Then, $f_\# : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.

61.1. Going up and going down

If $A \subseteq B$ is an integral extension, then $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.

Theorem 61.1.1.
$A \subseteq B$ an integral extension and $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n$ is a chain of prime ideals in A. Suppose there exists a chain of prime ideals $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m (m < n)$ in B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$. Then, $\mathfrak{q}$-chain can be extended to a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ of prime ideals in B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i \; \forall \; i$

Corollary 61.1.2.
If $A \subseteq B$ is an integral extension and prime ideals of A satisfy acc, then prime ideals of B also satisfy acc.

Definition 61.1.3.
An integral domain A is called normal (or integrally closed) if A is integrally closed in its fraction field.

Example 61.1.4.
$A = \mathbb{Z}$. Any UFD is normal. Normal does not imply UFD

Proposition 61.1.5.
Let $A \subseteq B$ be an inclusion of rings and let C be the integral closure of A in B. Let $S \subseteq A$ be a multiplicatively closed set. Then, $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Corollary 61.1.6.
Every localisation of a normal domain is a normal domain.

Example 61.1.7.
A normal implies $A_{\mathfrak{p}}$ normal for all $\mathfrak{p}$

Normalisation of A = integral closure of A in $\mathrm{Frac}(A)$

Exercise 61.1.8. *Is normalisation of A always finite over A?*

Example 61.1.9.

Proposition 61.1.10.
Let A be an integral domain. TFAE:

1. A is normal
2. $A_{\mathfrak{p}}$ is normal for all $\mathfrak{p} \in \mathrm{Spec}(A)$
3. $A_{\mathfrak{m}}$ is normal for all $\mathfrak{m} \in \mathrm{maxSpec}(A)$

Let $A \subseteq B$ be an inclusion of rings. $I \subseteq A$ an ideal. $x \in B$ is integral over I if there exists a monic polynomial $f(x) \in I[x]$ such that $f(x) = 0$.
Suppose $A \subseteq B$ is an extension and C the integral closure of A in B.

Proposition 61.1.11.
The integral closure of I in B is $\sqrt{IC}$

Corollary 61.1.12.
Integral closure of an ideal is a radical ideal.

Proposition 61.1.13.
$A \subseteq B$ be an inclusion of integral domains with A normal. Suppose $x \in B$ is integral over $I \subseteq A$. Then,

1. x is algebraic over $k = \mathrm{Frac}(A)$
2. If $t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in k[t]$ is the minimal polynomial of x over k, then $a_{i \in \sqrt{I}}$

Theorem 61.1.14.
$A \subseteq B$ an inclusion of integral domains with A normal. Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a descending chain of ideals in A. Let $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m (m < n)$ be a descending chain of prime ideals in B such that $\mathfrak{q}_i \cap A \mathfrak{p}_i \forall\ 1 \leq i \leq m$. Then, the $\mathfrak{q}$-chain can be extended to a chain of prime ideals $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m \supseteq \mathfrak{q}_{m+1} \supseteq \cdots \supseteq \mathfrak{q}_n$ such that $q_i \cap A = \mathfrak{p}_i\ \forall\ 1 \leq i \leq n$.

Theorem 61.1.15.
Let A be a normal domain with $\mathrm{Frac}(A) = k$ and L/k be a finite separable extension. Let $B \subseteq L$ be an integral closure of A in L. Then there exists a basis $v_1, \ldots, v_n$ of L such that $B \subseteq Av_1 \oplus \cdots \oplus Av_n$.

Corollary 61.1.16.
If A is Noetherian, then B is Noetherian. In fact, B is finite over A.

Proposition 61.1.17.
Suppose A is an integral domain integrally closed in its fraction field K, L is some finite separable extension of K. If B is integral closure of A in L, then B is finite A-module

Corollary 61.1.18.
In the prev. setup $L = \mathrm{Frac}(B)$

Remark 61.1.19.
In fact, the corollary is true if A is any domain (not necessarily integrally closed in K) and if L is any finite extension of K (not necessarily separable)

Proposition 61.1.20.
Let $f : A \to B$ be an integral extension of commutative rings. Then we get $f_\# : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ us a closed mapping.

Proposition 61.1.21.
Let $f : A \to B$ be a map of integral domains and an integral extension such that B is Noetherian. Then,

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

is quasi-finite (all fibers are finite)

61.2. Noether Normalisation Theorem

Theorem 61.2.1 (Noether Normalisation theorem)**.**
Let k be an infinite field and let $A = k[y_1, \dots, y_n]$ be a k-algebra (not necessarily a polynomial ring, the y_i's may have relations). Then, there exists $x_1, \dots, x_r \in A$ which have the following properties:

1. Each x_i is a linear combination of y_j's.
2. x_i's are algebraically independent over k.
3. A is integral over $k[x_1, \dots, x_r]$ (a polynomial ring)

Remark 61.2.2.

1. We do not need k to be infinite
2. Since A is integral and finite type over $k[x_1, \dots, x_r]$, then A is actually finite over the polynomial algebra $k[x_1, \dots, x_r]$

Exercise 61.2.3. *2,4,5,6,9,11,12,13,14,15 from Atiyah McDonald chapter 5*

62. Discrete Valuation Rings

62.1. Valuation Rings

Definition 62.1.1.
A Noetherian local ring $(A, \mathfrak{m})$ is called regular if $\mathfrak{m} = \langle f_1, \dots, f_r \rangle$ where $r = \dim(A)$

Definition 62.1.2.
Let B be an integral domain contained in a field k. Then B is called a valuation ring of k if for all $x \in k^\times$ we have $B \cap \{x, x^{-1}\} \neq \emptyset$

Proposition 62.1.3.
Let B be a valuation ring of k. Then,

1. B is local.
2. If $B \hookrightarrow B' \hookrightarrow k$, then B' is also a valuation ring
3. B is integrally closed

Let k be a field and Ω be an algebraically closed field. Then, Σ the set of all pairs (A, f) where A is a subring of k and $f : A \to \Omega$ is a ring homomorphism.
We give a partial order to Σ by $(A, f) \leq (A', f')$ if $A \subseteq A'$ and $f|'_A = f$.
By Zorn's lemma, Σ has a maximal element. Let (B, f) be the maximal element.

Lemma 62.1.4.
B is local

Lemma 62.1.5.
Let (B, f) be as above and let $x \in k^\times$. Let $B' = B[x]$ and let $\mathfrak{m}[x] = \mathfrak{m}B'$ where $\mathfrak{m} = \mathfrak{m}_B$. Then, either $\mathfrak{m}[x] \neq B[x]$ or $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$

Theorem 62.1.6.
B is a valuation ring.

Corollary 62.1.7.
Let $A \hookrightarrow k$ be a subring. Define $\bar{A}$ to the integral closure of A in k. Then,

$$\bar{A} = \bigcap_{B \subseteq A, B \text{valuation ring of } k} B = \tilde{A}$$

Definition 62.1.8.
An integral domain whose localisation at all prime ideals is a valuation ring is called a Prüfer domain.

Definition 62.1.9.
Let $A \hookrightarrow B$ be an inclusion of local rings. We say that B dominates $A (B \geq A)$ if $\mathfrak{m}_B \cap A = \mathfrak{m}_A (\mathfrak{m}_A B \subseteq \mathfrak{m}_B)$

Let k be a field and let Σ' be the set of all local subrings of k ordered by domination. Then, Zorn's lemma guarantees the existence of a maximal element.

Theorem 62.1.10.
Any maximal element of Σ' is a valuation ring of k.

Corollary 62.1.11.
Let k be a field and $A \hookrightarrow k$ be a local ring. Then, A is dominated by a valuation ring of k.

Remark 62.1.12.
A valuation ring of k is also called a place of k. $\mathrm{Spec}^*(k) =$ all places of k

Proposition 62.1.13.
Let A be an integral domain with $\mathrm{Frac}(A) = k$. TFAE:

1. A is a valuation ring of k
2. for all pairs of ideals $I, J \subseteq A$, one has either $I \subseteq J$ or $J \subseteq I$

Remark 62.1.14.
A is a valuation ring iff $\mathsf{I}(A)$ the set of all ideals of A is a totally ordered set

Corollary 62.1.15.
Let A be a valuation ring and $\mathfrak{p} \in \mathrm{Spec}(A)$. Then, $A/\mathfrak{p}$ and $A_{\mathfrak{p}}$ are valuation rings.

Corollary 62.1.16.
Let A be a valuation ring of k. Then, any subring of k containing A must be local.

62.2. Totally ordered abelian group

Let A be valuation ring of a field k. Let $U = A^\times$ then $U \hookrightarrow K^\times$. Let $\Gamma = K^\times/U$ and $\nu : K^\times \to \Gamma$ be quotient map. We define an order on Γ as follows:
Let $zeta, \eta \in \Gamma$, we say that $\eta \leq \zeta$ if there exists $a, b \in K^\times$ such that

1. $\nu(a) = \zeta, \nu(b) = \eta$
2. $ab^{-1} \in A$

Proposition 62.2.1.
$(\Gamma, \leq)$ is a totally ordered abelian group.

We have $\nu : K^\times \to \Gamma$ such that $\ker(\nu) = A^\times$, and
$A = \{a \in K^\times \mid \nu(a) \geq 0\} \cup \{0\}$

Exercise 62.2.2. *$\nu(x+y) \geq \min(\nu(x), \nu(y))$ for $x + y \in k^\times$*

Definition 62.2.3.
Let $(\Gamma, \leq)$ be a totally ordered abelian group and k be any field. Then a valuation ring is a group homomoprhism $\nu : k^\times \to \Gamma$ such that $\nu(x+y) \geq \min(\nu(x), \nu(y))$ for $x + y \in k^\times$

In this case, $\nu(k^\times)$ is called the value group of ν
$A = \{a \in k^\times : \nu(a) \geq 0\} \cup \{0\}$ is called the ring of integers of ν.

Proposition 62.2.4.
The ring of integers of a valuation on k is a valuation ring of k.

An integral domain A with $K = \mathrm{Frac}(A)$ is a valuation ring iff there exists a valuation on K whose ring of integers is A.

We know that valuations on $K \leftrightarrow$ places of the field

Set of all valuations on $K = RZ(K) =$ Riemann-Zariski space of K

Proposition 62.2.5.
Let A be a valuation ring with residue field F and let $A' \subseteq F$ be a valuation ring of F. Let

$$R = \{a \in A \mid a \pmod{\mathfrak{m}_A} \in A'\}$$

Then, R is a valuation ring of $K = \mathrm{Frac}(A)$

$$\begin{array}{ccccc} R = \phi^{-1}(A) & \hookrightarrow & A & \hookrightarrow & K \\ \downarrow & & \downarrow & & \\ A' & \hookrightarrow & F & & \end{array}$$

Exercise 62.2.6. $A' = \mathbb{F}_q[[t]], F = \mathbb{F}_q((t)), A = A'[[u]], K = \mathbb{F}_q((t,u))$

Proposition 62.2.7.
Let A be a local integral domain. TFAE:

1. A is a valuation ring
2. Every f.g. ideal of A is principal

Theorem 62.2.8.
1. Every totally ordered abelian group is the value group of a valuation of field
2. Totally ordered abelian group is torsion free
3. Every torsion free abelian group is a totally ordered abelian group
4. Suppose A is a valuation ring with valuation $\nu : K^\times \to \Gamma$. The rank of ν is the dimension of A.

Theorem 62.2.9.
ν has rank 1 iff the corresponding value group is a subgroup of $(\mathbb{R}, \leq)$

62.3. Discrete Valuation Rings

Definition 62.3.1.
Let $\nu : K^\times \twoheadrightarrow \mathbb{Z}$ be a valuation with usual order on $\mathbb{Z}$. Then, $\nu^{-1}(\mathbb{Z}_{\geq 0})$ is called a DVR.

Theorem 62.3.2.
Let A be an integral domain with function field $K \neq A$. TFAE:

1. A is DVR
2. A is a Noetherian valuation ring
3. A is a Noetherian local domain of dimension 1, which is normal
4. A is Noetherian local domain whose maximal ideal is principal
5. A is Noetherian local domain with maximal ideal $\mathfrak{m}$ and residue field $\|$ such that $\dim_{\|} \mathfrak{m}/\mathfrak{m}^2 = 1$
6. A is Noetherian local domain with maximal ideal $\mathfrak{m}$ such that every non-zero ideal is a power of $\mathfrak{m}$
7. A is a Noetherian local domain and there exists $x \in A$ such that every non-zero ideal of A is of the form $\langle x^n \rangle$

63. Primary decomposition

Let A be a commutative ring, and $\mathfrak{q} \subsetneq A$ be an ideal

Definition 63.0.1.
$\mathfrak{q}$ is called a primary ideal if for all $a, b \in A$ such that $ab \in \mathfrak{q}$, we must have either $a \in \mathfrak{q}$ or $b \in \sqrt{\mathfrak{q}}$.
Equivalently in $A/\mathfrak{q}$, every non-zero divisor is nilpotent.

$A \xrightarrow{f} B$, $\mathfrak{q} \subseteq B$ primary implies $f^{-1}(\mathfrak{q}) = \mathfrak{q}^c$ is also primary.

Suppose I has a primary decomposition. Then, I has a finite set of associated primes. Furthermore, if $X\mathrm{Spec}(A), X = \mathcal{V}(I)$ is closed, then Z has finitely many irreducible closed subsets $\{V_1, \ldots, V_n\} = \{\mathcal{V}(\mathfrak{p}_1), \ldots, \mathcal{V}(\mathfrak{p}_r)\}$ where $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \mathrm{Min}(I)$
Suppose I has a primary decomposition, $B = \mathrm{Min}(I) =$ minimal elements in the set $\mathrm{Ass}(I)$

Proposition 63.0.2.
$A =$ minimum elements of $\mathcal{V}(I) = \mathrm{Min}(I)$

Proposition 63.0.3.
Assume I has a primary decomposition, $\mathrm{Ass}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Then,

$$\bigcup_{i=1}^{r} \mathfrak{p}_i = \{x \in A \mid (I : x) \neq I\} = \{x \in A \mid x \pmod{\Gamma} \text{ is a zero divisor in } A/I\}$$

63.1. Primary ideals under localisation

Proposition 63.1.1.
$S \subseteq A$ multiplicatively closed set, $\mathfrak{q}$ a primary ideal with $\sqrt{\mathfrak{q}} = \mathfrak{p}$

1. If $S \cap \mathfrak{p} \neq \emptyset$ then $S^{-1}\mathfrak{q} = S^{-1}A$
2. If $S \cap \mathfrak{p} = \emptyset$ then $S^{-1}\mathfrak{q}$ is a $S^{-1}\mathfrak{p}$ primary ideal and $S^{-1}\mathfrak{q} \cap A = \mathfrak{q}$

Proposition 63.1.2.
Let $I = \bigcap \mathfrak{q}_i$ be a primary decomposition with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be numbered so that $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_r$ meet S and $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ do not meet S. Then,

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i \text{ and } S(I) = \bigcap_{i=1}^{m} \mathfrak{q}_i \tag{63.1}$$

are primary decomposition.

Proposition 63.1.3.
Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the minimal primes of I. Let $S = A \setminus (\bigcup_{i=1}^{s})$. Then, $S(I) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$

Suppose I has a primary decomposition, say

$$\begin{aligned} I &= \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \\ &= (\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s) \cap (q_{s+1} \cap \cdots \cap \mathfrak{q}_r) \end{aligned}$$

where the first s ones are minimal primes and $s+1$ to rth ones are embedded primes.

Definition 63.1.4.
We say that I is irreducible if $I = J \cap K$, then $I = J$ or $I = K$.

Theorem 63.1.5.
Suppose A is Noetherian. Then every ideal is finite intersection of irreducible ideals.

Proposition 63.1.6.
Every irreducible ideal is primary.

Corollary 63.1.7.
In a Noetherian ring, every ideal has a primary decomposition.

64. Dedekind domains

Proposition 64.0.1.
A is Noetherian integral domain of dimension 1. TFAE:

1. A is normal
2. Every primary ideal is a prime power
3. $A_{\mathfrak{p}}$ is a DVR for all non-zero prime ideal $\mathfrak{p}$.

Definition 64.0.2.
Let A be a Noetherian local domain of dimension 1. We say that A is a Dedekind domain if any of the equivalent conditions of the proposition holds.

Corollary 64.0.3.
In a Dedekind domain, every non-zero ideal has an unique factorisation as a finite product of prime ideals.

Remark 64.0.4.
A Dedekind domain is a f.g. algebra over a field is like an affine open subset of a Riemann surface.

Example 64.0.5.
$A = k[X], \operatorname{Spec}(A) = \mathbb{A}^1_k \xrightarrow{compactification} \mathbb{P}^1_k$

Proposition 64.0.6.
Let K be a number field and let $A = \mathcal{O}_K$. Then, A is a Dedekind domain.

Corollary 64.0.7.
Let A be a Dedekind domain and M a torsion free A-module. Then, M is flat.

64.1. Fractional Ideals

Let A be an integral domain with $\operatorname{Frac}(A) = K$, let M be an A-submodule

Definition 64.1.1.
We say that M is a fractional ideal if there exists $x \in A\backslash\{0\}$ such that $xM \subseteq A (M \subseteq Ax^{-1} \subseteq K)$

If M is a fractional ideal, we write

$$(A : M) = \{y \in K \mid yM \subseteq A\}$$

We say that $M \subseteq K$ is an invertible ideal if there exists a submodule $N \subseteq K$ such that $MN = NM = A$. We say that M is principal if $M = Ax^{-1}$ for some $x \neq 0 \in K$.

Proposition 64.1.2.
Suppose $M \subseteq K$ is a f.g. A-submodule. Then, M is a fractional ideal.

Proposition 64.1.3.
Suppose A is Noetherian. Let M be a fractional ideal of A. Then, M is a f.g. A-module.

In conclusion, if A is Noetherian, then

$$\{\text{Fractional ideals }\} \leftrightarrow \{\text{ f.g. } A\text{-submodules of } K\}$$

Suppose M is an invertible ideal, then there exists $N \subseteq K$ submodule such that $MN = A$

Proposition 64.1.4.
$N = (A : M)$

Proposition 64.1.5.
An invertible ideal is f.g. and hence fractional.

Remark 64.1.6.
The set of invertible ideals form an abelian group under multiplication. This is called the Picard group of A, denoted by $\mathrm{Pic}(A)$.

Proposition 64.1.7.
Let M be a fractional ideal of A. TFAE:

1. M is invertible
2. M is f.g. and $M_{\mathfrak{p}}$ is invertible for all prime ideals $\mathfrak{p}$
3. M is f.g. and $M_{\mathfrak{m}}$ is invertible for all maximal ideals $\mathfrak{m}$

Proposition 64.1.8.
Assume that A is a local domain. TFAE:

1. A is a DVR
2. Every fractional ideal of A is invertible.

Theorem 64.1.9.
Let A be an integral domain. Then, A is a Dedekind domain iff every fractional ideal of A is invertible.

Corollary 64.1.10.
In a Dedekind domain, the fractional ideals form an abelian group under multiplication whose identity is A

Corollary 64.1.11.
The group of fractional ideals is a free abelian group

Proposition 64.1.12.
Let A be a Dedekind domain. Then, A is a PID iff the class group of A (Picard group of A) is trivial iff A is a UFD.

Theorem 64.1.13.
Let A be a number ring. Then, $\mathcal{C}\!\updownarrow\!(A)$ is finite.

Remark 64.1.14.
It is known that every finite abelian group is the class group of a Dedekind domain, but whether it is the class group of a number ring is not yet answered.

Proposition 64.1.15.
Let A be a Noetherian integral domain. Let M be a f.g. A-module. Then, M is projective of rank 1 iff M is an invertible ideal.

Theorem 64.1.16.
Let A be a Dedekind domain and $I \subseteq A$ a non-zero ideal. Then, I is generated by atmost 2 elements.

Exercise 64.1.17. *Prove that a semilocal Dedekind domain is a PID (Show that class group is trivial)*

65. Completions

65.1. Topological groups

Definition 65.1.1.
A topological group is a topological space G such that the two maps

$$\begin{array}{lll} G \times G \to G & G & \to G \\ (x,y) \mapsto xy & x & \mapsto x^{-1} \end{array}$$

are continuous.

Proposition 65.1.2.
G is Hausdorff iff $\{1\}$ is closed in G

Let H be the intersection of all open neighbourhoods of 1

Proposition 65.1.3.
1. H is a subgroup
2. $H = \overline{\{1\}}$
3. G/H is Hausdorff
4. G is Hausdorff iff $H = \{1\}$

Definition 65.1.4.
Let (a_n) be a sequence in G (written additively). We say that this sequence is Cauchy if for all neighbourhoods U of 0 there exists $s = s(U) \in \mathbb{Z}$ such that $a_m - a_n \in U \ \forall\ m, n \geq s$.

We say that $(a_n) \sim (b_n)$ if $a_n - b_n \to 0$ as $n \to \infty$

Let $\hat{G}$ be the set of all equivalence classes of Cauchy sequences in G. Then, $\hat{G}$ is an abelian group and there exists a homomorphism $\phi : G \to \hat{G}$ such that $a \mapsto (a)$. The Kernel of this map is clearly H. We say that G is complete if $G \cong \hat{G}$.

Next, assume that G has a filtration by subgroups

$$(*) G = G_0 \supseteq G_1 \supseteq \cdots$$

Then $(*)$ defined a unique topology on G such that (G_n) becomes a system of neighbourhoods of zero (the subspace topology)

Next, consider the system (G/G_n) with $G_i \supseteq G_{i+1}$ and a map

$$G/G_{n+1} \xrightarrow{\gamma_{n+1}} G/G_n$$

This clearly gives us an inverse system and thus we have

$$\hat{G} = \varprojlim_n G/G_n$$

$$G \xrightarrow{\phi} \widehat{G} \hookrightarrow \prod_n G/G_n \longrightarrow G/G_n \qquad (\lambda_n)$$

In a topological group, if we quotient by an open subgroup, we get a discrete topology and thus,

$$G \xrightarrow{\phi} \widehat{G} \hookrightarrow \prod_n G/G_n \longrightarrow G/G_n \qquad (\psi)$$

with ψ continuous, which implies ϕ is continuous and this concept of $\widehat{G}$ is same as the previous one.
In general, if $I \subseteq R$ is an ideal, we can take the filtration

$$R = I_0 \supseteq I \supseteq I^2 \supseteq \cdots$$

Example 65.1.5.
$R = A[t], I = \langle t \rangle, G_n = I^n$ then $\widehat{A[t]} = A[[t]]$

Lemma 65.1.6.
Suppose

$$0 \longrightarrow \{A_n\} \xrightarrow[\alpha_n]{} \{B_n\} \xrightarrow[\beta_n]{} \{C_n\} \longrightarrow 0$$

is an exact sequence of inverse systems. Then,

$$0 \longleftarrow \varprojlim_n A_n \xleftarrow{\alpha} \varprojlim_n B_n \xleftarrow{\beta} \varprojlim_n C_n \longleftarrow 0$$

is exact. Furthermore, β is injective if $\{A_n\}$ is a surjective inverse system.

Lemma 65.1.7.
If

$$0 \longrightarrow G' \xrightarrow[\alpha]{} G \xrightarrow[\beta]{} G'' \longrightarrow 0$$

is an exact sequence where G is a topological group and G' has subspace topology and G'' has quotient topology. Then,

$$0 \longrightarrow \widehat{G'} \xrightarrow[\alpha^*]{} \widehat{G} \xrightarrow[\beta^*]{} \widehat{G''} \longrightarrow 0$$

is exact.

Corollary 65.1.8.

$$0 \longrightarrow \{G'/G' \cap G_n\} \longrightarrow \{G/G_n\} \longrightarrow \{G/G'\} \longrightarrow 0$$

is exact.

Corollary 65.1.9.
For all n, $\widehat{G_n} \hookrightarrow \widehat{G}$ and $G/G_n \xrightarrow{\sim} \widehat{G}/\widehat{G_n}$

Corollary 65.1.10.
$\widehat{\widehat{G}} \xrightarrow{\sim} G$

65.2. I-adic completion

Let A be a commutative ring, $I \subseteq A$ an ideal. $\{I^n A\}$ defines the I-adic topology on A. $\phi : A \to \widehat{A}$ a map.

If M is a A-module, then $\{I^n M\}$ defines a topology on M called the I-adic topology on M and

$$M \longrightarrow \widehat{M}$$

is the I-adic completion.

- $\widehat{M}$ is a $\widehat{A}$-module.
- A/I^n acts on $M/I^n M$
- $\widehat{A} = \varprojlim_n A/I^n$ acts on $\varprojlim_n M/I^n M$

Definition 65.2.1. 1. We say that M is a I-filtration if

$$IM_n \subseteq M_{n+1} \; \forall \; n$$

2. We say that M is I-stable if

$$IM_n = M_{n+1} \; \forall \; n >> 0$$

Remark 65.2.2.
$(1) \Rightarrow I^n M \subseteq M_n \; \forall \; n \Rightarrow I$-adic topology is finer than the M topology.

65.3. Graded Rings

Definition 65.3.1.
A graded ring is a commutative ring A with a decomposition of $(A, +)$

$$A = \bigoplus_{m \geq 0} A_m$$

such that $A_m A_n \subseteq A_{m+n}$

This means A_0 is a subring of A and A is an A_0-algebra.

Definition 65.3.2.
Suppose A is a graded ring. An A-module M is called graded if

$$M = \bigoplus_{n \geq 0} M_n$$

as abelian group such that $A_n M_m \subseteq M_{n+m} \; \forall \; n, m$

Definition 65.3.3.
$\phi : M \to N$ map of graded A-modules is an A-linear map such that $\phi(M_m) \subseteq N_m \; ; \forall \; m$

65.4. Projective scheme

Theorem 65.4.1.
Let $A = \bigoplus_n A_n$ be a graded ring. TFAE:

1. A is Noetherian
2. A_0 is Noetherian and A is a f.g. A_0-algebra

65.5. Rees Algebra

Definition 65.5.1.
Let $I \subseteq A$ not necessarily graded, then the Rees algebra of I , denoted by $A(I)$ is defined as

$$A(I) = \bigoplus_{n \geq 0} I^n$$

such that $I^n I^m \subseteq I^{n+m}$

Suppose M is an A-module with a filtration M which is a I-filtration. Then,

$$M^* = \bigoplus_{n \geq 0} M_n$$

implies M^* becomes an $A(I)$-module.

Lemma 65.5.2.
If A is Noetherian. TFAE:

1. $\{M\}$ is I-stable
2. M^* is a f.g. $A(I)$-stable

Theorem 65.5.3.
If M is I-stable on M, then $\{M \cap M'\}$ is also I-stable on M' if M is f.g. A-module.

Theorem 65.5.4.
If

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence of f.g. A-modules. Then,

$$0 \longrightarrow \widehat{M'} \longrightarrow \widehat{M} \longrightarrow \widehat{M''} \longrightarrow 0$$

is exact.

Theorem 65.5.5.

$$\widehat{A} \otimes_A M \xrightarrow{\sim} \widehat{M} \tag{65.1}$$

Corollary 65.5.6.
$\widehat{A}$ is a flat A-algebra.

Theorem 65.5.7.
1. $\widehat{I} \simeq I\widehat{A} \simeq I \otimes_A \widehat{A}$
2. $\widehat{I^n} \simeq (\widehat{I})^n$
3. $\dfrac{I^n}{I^{n+1}} \simeq \dfrac{\widehat{I}^n}{\widehat{I}^{n+1}}$
4. $\widehat{I} \subseteq J(\widehat{A})$

Proposition 65.5.8.
Assume that $(A, \mathfrak{m})$ is local. Then, $(\widehat{A}, \widehat{\mathfrak{m}})$ is local and $A/\mathfrak{m} \simeq \widehat{A}/\widehat{\mathfrak{m}}$

Theorem 65.5.9.
Suppose A is Noetherian and $I \subseteq A$ ideal and M a f.g. A-module. Then,

$$\begin{aligned}\ker(M \to \widehat{M}) &= \bigcap_{n\geq 1} I^n M \\ &= \{x \in M \mid x \text{ is annihilated by some element of } 1 + I\}\end{aligned}$$

Corollary 65.5.10.
Suppose A is an integral domain. Then,

$$\bigcap_{n\geq 0} I^n = \{0\}$$

Theorem 65.5.11.
If $(A, \mathfrak{m})$ is Noetherian and local. Then, for any f.g. A-module M, the $\mathfrak{m}$-adic topology on M is Hausdorff.

66. Dimension Theory

Part VII.

Algebraic Number Theory

67. Dedekind Domains

68. Splitting of primes

69. Finiteness of class number

70. Unit theorem

71. Cyclotomic Fields and Fermat's last theorem

72. Local Fields

73. Global Fields

74. Kronecker Weber

75. Adéles and Idéles

Part VIII.

Galois Theory

76. Fundamental theorem of Galois Theory

77. Infinite Galois Theory

78. Finite Fields

79. Cyclotomic Fields

Part IX.

Representation theory

80. Introduction

81. Character theory

82. Wedderburn theorem

83. Induced characters

84. Brauer Induction theorem

Part X.

Miscellaneous

85. Galois representations

86. Artin L-functions

87. Riemann hypothesis for curves over finite fields

88. Nèron models

89. Nagata-Zariski-Lipman

The objective is to prove the following theorem.

Theorem 89.0.1 (Nagata-Zariski-Lipman)**.**
Let $(A, \mathfrak{m})$ be a complete Noetherian local ring with $\mathbb{Q} \subseteq A$. Suppose that $x_1, \ldots, x_r \in \mathfrak{m}$ and $D_1, \ldots, D_r \in \mathrm{Der}(A)$ are elements satisfying $\det(D_i x_j) \notin \mathfrak{m}$. Then,

1. There exists a subring $C \subseteq A$ such that

$$A = C[[x_1, \ldots, x_r]] \simeq C[[X_1, \ldots, X_r]] \tag{89.1}$$

   Therefore x_i are analytically independent over C and A is I-smooth over C where $I = \sum_{i=1}^{r} Ax_i$ and therefore also $\mathfrak{m}$-smooth over C.

2. If $\mathfrak{g} = \sum_{i=1}^{r} AD_i$ is a Lie algebra ($[D_i, D_j] \in \mathfrak{g}\ \forall\ i, j$), then we can take C to be

$$C = \{a \in A : D_1 a = D_2 a = \cdots = D_r a = 0\} \tag{89.2}$$

89.1. Preliminaries

89.2. Proof