University of Chinese Academy of Sciences

The Analytic Class Number formula & The Weak Mordell-Weil Theorem

Yi Wei

July 23, 2018

Abstract

This paper is developed based on breif notes of what I have prepared for the Algebraic Number Theory Seminar in 2018 spring semester. The first section shows a complete proof of a weak form of analytic class number formula and introduces some results and concepts to prove the formula completely using Tate's theory. The second section exhibits the weak Mordell-Weil theorem but beforehand introduces concepts and notions from the theory of elliptic curves. Many facts are shown without proof due to its complexity and in many cases I consult to references.

Many thanks to Professor Tian Ye for revising my lecture notes and my classmates for listening.

Contents

1 The Analytic Class Number Formula

In this section we will use tools from analysis to provide an explicit formula for the class number of a number field. The main idea and process follows the article [1].

1.1 Basic Notations And Definitions in Number Theory

- K: number field of degree $n = [K : \mathbb{Q}]$ with ring of integers $\mathcal{O}_K$.
- D_K: Discriminent of K, i.e., if $\{\alpha_1, \cdots, \alpha_n\}$ is the integral basis of K. $D_K = d_K(\alpha_1, \cdots, \alpha_n) = |\det(\sigma_i(\alpha_j)_{1\le i,j\le n})|^2$.
- $\mathcal{I}_K$: The set of all non-zero integral ideals of K.
- $\mathcal{C}_K$: The class group of K. $h_K = |\mathcal{C}_K|$
- r_1: The number of real embeddings, denoted as $\sigma_1, \cdots, \sigma_{r_1}$.
- r_2: The number of pairs of complex embeddings, denoted as $\sigma_{r_1+1}, \bar{\sigma}_{r_1+1} \cdots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$.
- $\mathcal{O}_K^\times$: The group of units of K. By Dirichlet's Theorem, $\mathcal{O}_K^\times \cong W_K \times \mathbb{Z}^r$, where $r = r_1 + r_2 - 1$. Let $\{\epsilon_1, \cdots, \epsilon_r\}$ be the generators of the free abelian subgroup. W_K is the group of roots unity of K. Its size is denoted as ω_K.
- Define a group homomorphism $l : \mathcal{O}_K^\times \to \mathbb{R}^{r_1+r_2}$ as $\alpha \mapsto (\lambda_i \log|\sigma_i(\alpha)|)$, where $\lambda_i = \begin{cases} 1, & 1 \le i \le r_1 \\ 2, & r_1 + 1 \le i \le r_1 + r_2. \end{cases}$ Let $l(\epsilon_i) = (y_{i,1}, \cdots, y_{i,r+1})$, then $R(\epsilon_1, \cdots, \epsilon_r) := |\det(y_{i,j})_{1\le i,j\le r}|$, which is independent of the choice of the basis, denoted as R_K.
- (Dedekind zeta function) For any number field K, define for $s > 1$:

$$\zeta_K(s) = \sum_{\mathfrak{a}\in\mathcal{I}_K} \mathrm{N}(\mathfrak{a})^{-s} \qquad \text{where } \mathrm{N}(\mathfrak{a}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| \text{ is the norm of an ideal.}$$

The main result we will prove is the following theorem.

Theorem 1.1. *$\zeta_K(s)$ converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, and*

$$\lim_{s\to 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{\omega_K |D_K|^{\frac{1}{2}}}$$

Remark 1.1. Notice that it is a weak form of the analytic class number formula. As soon as analytical continuation of $\zeta_K(s)$ to the whole complex plane is completed, which shows that $s = 1$ is the only simple pole of $\zeta_K(s)$, then its residue conincides with the limit.

At the first place, it is rather confusing what range the summation actually cover. A more basic question can be asked like this: how does integral ideals distribute geometrically in $\mathcal{I}_K$ and how can we calculate it.

1.2 Skethch of Proof And Some Elementry Examples

Split the sum as

$$\zeta_K(s) = \sum_{A\in\mathcal{C}_K} \Big(\sum_{\mathfrak{a}\in A\cap\mathcal{I}_K} \mathrm{N}(\mathfrak{a})^{-s} \Big).$$

And define $f_A(s) = \sum_{\mathfrak{a}\in A\cap\mathcal{I}_K} \mathrm{N}(\mathfrak{a})^{-s}$. We will evaluate each $\lim_{s\to 1^+}(s-1)f_A(s)$ seperately. First, we give an observation: Take $0 \ne \mathfrak{b}$ integral ideal such that $\mathfrak{b} \in A^{-1}$, then $\forall \mathfrak{a} \in A \cap \mathcal{I}_K$, $\mathfrak{ab}$ is principal, i.e., $\mathfrak{ab} = (\alpha)$ for some $\alpha \in K^\times$. On the other hand, any principal ideal (α) with $(\alpha) \subseteq \mathfrak{b}$, there exists an integral ideal $\mathfrak{a} \in A$, such that $\mathfrak{ab} = (\alpha)$ since $\mathcal{O}_K$ is a dedekind domain. Then multiplication by $\mathfrak{b}$ gives a bijection between integral ideals in A and principal ideals divisible by $\mathfrak{b}$. And $\alpha\mathcal{O}_K = \alpha\mathcal{O}_K \Leftrightarrow \alpha^{-1}\beta \in \mathcal{O}_K^\times$. Thus it shows that there is a 1-1 correspondence bewteen the set $\{A \cap \mathcal{I}_K\}$ and the set $\{\alpha \in K^\times \,|\, \alpha\mathcal{O}_K \subseteq \mathfrak{b}\}/\mathcal{O}_K^\times$. For the convenience of notation, in the following contexts, we fix an integral ideal $\mathfrak{b} \in A^{-1}$ and define

$$\mathcal{A}_\mathfrak{b} = \{\alpha \in K^\times \,|\, \alpha\mathcal{O}_K \subseteq \mathfrak{b}\}/\mathcal{O}_K^\times.$$

Notice that $\alpha^{-1}\beta \in \mathcal{O}_K^\times$ implies $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$ and moreover, $|\mathrm{N}(\alpha)| = \mathrm{N}(\alpha\mathcal{O}_K)$ for all $\alpha \in K^\times$, which we will prove afterwards. Now we may simplify the range of sumation as

$$f_A(s) = \mathrm{N}(\mathfrak{b})^s \sum_{\alpha\in\mathcal{A}_\mathfrak{b}} \mathrm{N}(\alpha\mathcal{O}_K)^{-s} = \mathrm{N}(\mathfrak{b})^s \sum_{\alpha\in\mathcal{A}_\mathfrak{b}} |\mathrm{N}(\alpha)|^{-s}$$

In order to get inspired to know what $\mathcal{A}_\mathfrak{b}$ looks like in general, we show some examples as $K = \mathbb{Q}$, real quadratic and imaginary quadratic field.

Example 1. $K = \mathbb{Q}$, let $\mathfrak{b}$ be $\mathbb{Z}$, then $\mathcal{A}_\mathfrak{b} = \{\alpha \in \mathbb{Q}^\times \,|\, (\alpha) \subseteq \mathbb{Z}\}/\mathbb{Z}^\times = \mathbb{Z}_{>0}$.

Example 2. $K = \mathbb{Q}(\sqrt{d}), d > 0$ squre free. Then $\mathcal{O}_K^\times = \{\pm 1\} \times \langle\epsilon\rangle$ by Dirichlet's unit theorem, where ϵ is the fundamental unit. And $\mathcal{A}_\mathfrak{b} = \{\alpha \in \mathbb{Q}(\sqrt{d})^\times \,|\, (\alpha) \subseteq \mathfrak{b}\}/\{\pm 1\} \times \langle\epsilon\rangle$. Notice that $\psi(\mathfrak{b})$ is a lattice in $\mathbb{R}^2$, denoted as Γ. And we will show that after a reasonable choice of representatives of equivalence class in $\mathcal{A}_\mathfrak{b}$, $\psi(\alpha) \in \psi(\mathfrak{b}) \cap X = \Gamma \cap X$, $\forall \alpha \in \mathcal{A}_\mathfrak{b}$, where X is a cone. Let us consider the following maps.

Define injective map $\psi : K \to \mathbb{R}^2$ as $\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha))$ and define $\eta : (\mathbb{R}^\times)^2 \to \mathbb{R}^2$ as $(a,b) \mapsto (\log|a|, \log|b|)$. First, by the effect of $\{\pm 1\}$, we may choose $\psi(\alpha) \in \mathbb{R}_{>0} \times \mathbb{R}$. Second, since ϵ is a unit, $\eta\circ\psi(\epsilon) = (a, -a) \in \mathbb{R}^2$. Let $\lambda = (1,1)$, then $\eta\circ\psi(\alpha) = c\lambda + c_1\eta\circ\psi(\epsilon)$. And $\eta\circ\psi(\alpha\cdot\epsilon^n) = c\lambda + (c_1+n)\eta\circ\psi(\epsilon)$. Therefore in order to erase the effect of $\langle\epsilon\rangle$, we shall choose α such that $\eta\circ\psi(\alpha) = c\lambda + c_1\eta\circ\psi(\epsilon)$ with $0 \leqslant c_1 < 1$. Let X be a cone defined as follows: 1) $X \subseteq \mathbb{R}_{>0} \times \mathbb{R}$; 2) $\forall x \in X, \eta(x) = c\lambda + c_1\eta\circ\psi(\epsilon)$, with $0 \leqslant c_1 < 1$. Actually, X is a cone. Indeed, $\eta(\xi\cdot x) = (\log\xi + c)\lambda + c_1\eta\circ\psi(\epsilon) = \log\xi\lambda + \eta(x) \in X, \forall \xi > 0, x \in X$. Therefore, $\psi(\alpha) \in \Gamma \cap X$.

Remark 1.2. From Example 2, we may guess that the elements in $\mathcal{A}_\mathfrak{b}$ is explicitly those elements $\alpha \in K^\times$ such that $\psi(\alpha) \in \Gamma \cap X$ for some cone X and $\Gamma = \psi(\mathfrak{b})$ a lattice. In this sense, we can write $\mathcal{A}_\mathfrak{b}$ in Example 1 as $\mathcal{A}_\mathfrak{b} = \mathbb{Z} \cap \mathbb{R}_{>0}$, where $\mathbb{R}_{>0}$ is a cone, and $\mathbb{Z}$ is a lattice in $\mathbb{R}$.

Example 3. $K = \mathbb{Q}(\sqrt{d}), d < 0$ squre free. Then $\mathcal{O}_K^\times = W_K$ by Dirichlet's unit theorem. Define the similar maps as above. Define $\psi : K \to \mathbb{C}$ as $\alpha \mapsto \alpha$ and define $\eta : \mathbb{C}^\times \to \mathbb{R}$ as $a \mapsto 2\log|a|$. First, $\psi(\mathfrak{b})$ is a lattice in $\mathbb{C}$, denoted as Γ. As we know W_K is a cyclic group with size ω_K generated by $e^{i2\pi/\omega_K}$. Notice that multipication by $e^{i2\pi/\omega_K}$ add $2\pi/\omega_K$ to the argument of a complex number. Therefore we may choose $\alpha \in K^\times$ such that $0 \leqslant \arg(\psi(\alpha)) < \frac{2\pi}{\omega_K}$. Let $X \subseteq \mathbb{C}$ be defined as follows: $\forall x \in X, 0 \leqslant \arg(x) < \frac{2\pi}{\omega_K}$. X is a cone, indeed, $0 \leqslant \arg(\xi\cdot x) = \arg(x) < \frac{2\pi}{\omega_K}, \forall \xi > 0, x \in X$. Therefore, $\psi(\alpha) = \Gamma \cap X$, where $\Gamma = \psi(\mathfrak{b})$, X is a cone.

1.3 General Cases

Having those examples in mind, it is enough to explore the general cases. In fact, the general case is a combination of Example 2 and Example 3. Let K be a number field, $[K : \mathbb{Q}] = n = r_1 + 2r_2$, with real and complex embedding $\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}\cdots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$ and $\{\epsilon_1, \ldots, \epsilon_r\}$ fundamental units, where $r = r_1 + r_2 - 1$. Fix $\mathfrak{b}$ an integral ideal and let $\mathcal{A}_\mathfrak{b} = \{\alpha \in K^\times \,|\, \alpha\mathcal{O}_K \subseteq \mathfrak{b}\}/\mathcal{O}_K^\times$. Define maps $\psi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as $\alpha \mapsto (\sigma_i(\alpha))_{1\leqslant i\leqslant r_1+r_2}$ and $\eta : (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$ as $(x_1, \ldots, x_{r_1+r_2}) \mapsto (\lambda_i \log|x_i|)$, where $\lambda_i = \begin{cases} 1, & 1 \le i \le r_1 \\ 2, & r_1 + 1 \le i \le r_1 + r_2. \end{cases}$ For convenience, we denote $\eta\circ\psi|_{K^\times} = l$ and set $\lambda = (1, \ldots, 1; 2, \ldots, 2)$. Since $\{\epsilon_1, \ldots, \epsilon_r\}$ are fundamental units, $\{l(\epsilon_i)\}$ are linearly independent and $\sum_{j=1}^{r_1+r_2} l_j(\epsilon_i) = 0$, $\forall l(\epsilon_i)$. It is clear that $\{\lambda, l(\epsilon_i)_{1\leqslant i\leqslant r}\}$ is a basis in $\mathbb{R}^{r_1+r_2}$. Then

$$\eta(x) = c\lambda + \sum_{i=1}^{r} c_i l(\epsilon_i), \qquad \sum_{j=1}^{r_1+r_2} \eta_j(x) = nc \qquad \forall x \in (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$$

Define $\|x\| = |x_1|\cdots|x_{r_1}| \cdot |x_{r_1+1}|^2\cdots|x_{r_1+r_2}|^2$ for all $x \in (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. Note that for all $\alpha \in K^\times$, $|\mathrm{N}(\alpha)| = \|\psi(x)\|$, thus $c = \log\|x\|/n$.

Definition 1.1. Let X to be a cone in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ consisting of all x satisfying

1. $\|x\| \neq 0$;
2. $\forall 1 \leqslant i \leqslant r_1 + r_2 - 1, \qquad 0 \leqslant c_i < 1$;
3. $0 \leqslant \arg(x_1) < \frac{2\pi}{\omega_K}$, x_1 is the first component of x.

Indeed, $\forall \xi > 0, \forall x \in X, \eta(\xi \cdot x) = \eta(\xi) + \eta(x) = \log \xi\lambda + \eta(x)$, $\arg((\xi \cdot x)_1) = \arg(x_1)$.

Remark 1.3. $r_1 \neq 0 \Rightarrow K \hookrightarrow \mathbb{R}$ and $W_K = \{\pm 1\}$. Thus 3. coincides with $x_1 > 0$.

We want to show that $\psi(\mathcal{A}_{\mathfrak{b}}) = \psi(\mathfrak{b}) \cap X$ by the following lemma.

Lemma 1.1. For any $\alpha \in K^\times$, then exactly one member of $\alpha\mathcal{O}_K^\times$ has image in X.

Proof. To show this, we will show that given $y \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with nonzero norm, y can be uniquely written as $y = x \cdot \psi(\epsilon)$, and $x \in X, \epsilon \in \mathcal{O}_K^\times$. First, write $\eta(y) = c\lambda + c_1 l(\epsilon_1) + \ldots + c_r l(\epsilon_r)$. Split each $c_i = m_i + \mu_i$, where $m_i \in \mathbb{Z}$ and $0 \leqslant \mu_i < 1$. Write $u = \epsilon_1^{m_i} \cdots \epsilon_r^{m_r}$ and define $z = y \cdot \psi(u^{-1})$, which has coefficients of each $l(\epsilon_i)$ in the correct range. Indeed

$$\begin{aligned}
\eta(z) &= \eta(y) + \eta \circ \psi(u^{-1}) = \eta(y) + l(u^{-1}) \\
&= c\lambda + c_1 l(\epsilon_1) + \ldots + c_r l(\epsilon_r) - m_1 l(\epsilon_1) - \ldots - m_r l(\epsilon_r) \\
&= c\lambda + \mu_1 l(\epsilon_1) + \ldots + \mu_r l(\epsilon_r).
\end{aligned}$$

Now we can correct $\arg(z_1)$. Let r be the unique integer such that $0 \leqslant \arg(z_1) - \frac{2\pi r}{\omega_K} < \frac{2\pi}{\omega_K}$ and choose a root of unit ω such that $\sigma_1(\omega) = e^{2\pi/\omega_K}$. Then $z \cdot \psi(\omega^{-r}) = y \cdot \psi(u^{-1}) \cdot \psi(\omega^{-r}) \in X$. So we conclude that if this element is called x, then $y = x \cdot \psi(u \cdot \omega^r)$ as desired, and clearly this construction must be unique. □

Now we have done a wonderful correspondence that transforms $\zeta_K(s)$ geometrically. And the summation refined into a more simple way:

$$f_A(s) = \mathrm{N}(\mathfrak{b})^s \sum_{\alpha \in \mathcal{A}} \mathrm{N}(\alpha)^{-s} = \mathrm{N}(\mathfrak{b})^s \sum_{x \in \Gamma \cap X} \|x\|^{-s}.$$

Then we turn to analyse functions on cones. Notice that at first we get a cone in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, for the meantime this is a cone in $\mathbb{R}^n$. We calculate $\lim_{s \to 1^+} (s-1) f_A(s)$ by calculating the general case.

1.4 Main lemma

Lemma 1.2. Let X be a cone in $\mathbb{R}^n$ and define a function $F : X \to \mathbb{R}_{>0}$ such that $x \in X$ and $\xi > 0$ implies $F(\xi \cdot x) = \xi^n F(x)$, and define $\mathcal{F} = \{x \in X : F(x) \leqslant 1\}$ with $v = vol(\mathcal{F}) > 0$. Also, let $\Gamma \subseteq \mathbb{R}^n$ be a lattice with covolume $\Delta = covol(\Gamma)$. Then

$$\zeta_{F,\Gamma}(s) = \sum_{x \in \Gamma \cap X} F(x)^{-s}$$

converges on Re(s)>1, and has $\lim_{s \to 1^+} (s-1)\zeta_{F,\Gamma}(s) = \dfrac{v}{\Delta}$.

As soon as the lemma is proved, we will define F to be $\|\cdot\|$ on $X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ and prove $\Delta = \mathrm{N}(\mathfrak{b})|D_K|^{1/2}$ and $v = \dfrac{2^{r_1}(2\pi)^{r_2} R_k}{\omega_K}$.

The proof of Lemma 1.2. For any positive real number r, $vol(\frac{1}{r}\Gamma) = \frac{\Delta}{r^n}$. Thus

$$\begin{aligned}
v &= vol(\mathcal{F}) = \lim_{r \to \infty} \left(\frac{\Delta}{r^n} \cdot \# \left\{ \frac{1}{r}\Gamma \cap \mathcal{F} \right\} \right) \\
&= \Delta \lim_{r \to \infty} \frac{\#\{\frac{1}{r}\Gamma \cap \mathcal{F}\}}{r^n}
\end{aligned}$$

By the requirements on F, $\#\left\{\frac{1}{r}\Gamma\cap\mathcal{F}\right\}=\#\{x\in\Gamma\cap X:F(x)\leqslant r^n\}$. Label the points of $\Gamma\cap X$ so that $0\leqslant F(x_1)\leqslant F(x_2)\leqslant\ldots$ and define $r_k=F(x_k)^{1/n}$. If we define $\gamma(r)=\#\left\{\frac{1}{r}\Gamma\cap\mathcal{F}\right\}$. Then by the choice of label we have $\forall\epsilon>0$, $\gamma(r_k-\epsilon)<k\leqslant\gamma(r_k)$. Therefore,

$$\frac{\gamma(r_k-\epsilon)}{(r_k-\epsilon)^n}\cdot\left(\frac{r_k-\epsilon}{r_k}\right)^n<\frac{k}{r_k^n}\leqslant\frac{\gamma(r_k)}{r_k^n}.$$

Since $r_k^n=F(x_k)$, taking the limit yields $\lim\limits_{k\to\infty}\frac{k}{r_k^n}=\frac{v}{\Delta}$. Write $\zeta_{F,\Gamma}(s)=\sum\limits_{k=1}^{\infty}F(x_k)^{-s}$. Now give $\forall\epsilon>0$, there exists k_0, such that $\forall k>k_0$, we have

$$\frac{v}{\Delta}-\epsilon<\frac{k}{r_k^n}=\frac{k}{F(x_k)}<\frac{v}{\Delta}+\epsilon\quad\Rightarrow\quad\left(\frac{v}{\Delta}-\epsilon\right)^s\cdot\frac{1}{k^s}<\frac{1}{F(x_k)^s}<\left(\frac{v}{\Delta}+\epsilon\right)^s\cdot\frac{1}{k^s}.$$

Summing over all $k>k_0$,

$$\left(\frac{v}{\Delta}-\epsilon\right)^s\cdot\sum_{k=1}>k_0\frac{1}{k^s}<\sum_{k=1}>k_0\frac{1}{F(x_k)^s}<\left(\frac{v}{\Delta}+\epsilon\right)^s\cdot\sum_{k>k_0}\frac{1}{k^s}.$$

Therefore $\zeta_{F,\Gamma}(s)$ converges for $s>1$. If $s=a+ib\in\mathbb{C}$, with $a>1$. Then

$$\left|\frac{1}{F(x_k)^s}\right|=\left|\frac{1}{F(x_k)^{a+ib}}\right|=\left|\frac{1}{F(x_k)^a}\right|\cdot\left|e^{-ib\log F(x_k)}\right|=\left|\frac{1}{F(x_k)^a}\right|.$$

$$\left|\zeta_{F,\Gamma}(s)\right|=\left|\sum_{k=1}^{\infty}\frac{1}{F(x_k)^s}\right|\leqslant\sum_{k=1}^{\infty}\left|\frac{1}{F(x_k)^s}\right|=\left|\frac{1}{F(x_k)^a}\right|.$$

Therefore $\zeta_{F,\Gamma}(s)$ converges for $\mathrm{Re}(s)>1$. Moreover, $(s-1)\sum\limits_{k>k_0}\frac{1}{F(x_k)^s}$ has the same limit as $(s-1)\zeta_{F,\Gamma}(s)$ as s approach 1(since s=1 is a pole of both function $(s-1)\sum\limits_{k>k_0}\frac{1}{F(x_k)^s}$ and $(s-1)\zeta_{F,\Gamma}(s)$, and the difference between them is only finitely many items). Therefore we have:

$$\left(\frac{v}{\Delta}-\epsilon\right)\cdot\mathrm{Res}_{s=1}\zeta(s)\leqslant\varliminf_{s\to1^+}(s-1)\zeta_{F,\Gamma}(s)\leqslant\varlimsup_{s\to1^+}(s-1)\zeta_{F,\Gamma}(s)\leqslant\left(\frac{v}{\Delta}+\epsilon\right)\mathrm{Res}_{s=1}\zeta(s).$$

Since the choice of ϵ is random, we obtain that the limit exists and $\lim_{s\to1^+}(s-1)\zeta_{F,\Gamma}(s)=\frac{v}{\Delta}$. ☐

1.5 Calculation

Now every thing is perfect. The remaining part of this section is to calculate and verify the propostion we claimed before.

Proposition 1.1. *Assume $\alpha\in\mathcal{O}_K$, then $|\mathrm{N}(\alpha)|=\mathrm{N}(\alpha\mathcal{O}_K)$*

Proof. If $\{\omega_1,\ldots,\omega\}$ is the integral basis of $\mathcal{O}_K$, then $\{\alpha\omega_1,\ldots,\alpha\omega_n\}$ is the integral basis of $\alpha\mathcal{O}_K$. Then

$$\left(\prod_{i=1}^{n}\sigma_i(\alpha)\right)^2\cdot\mathrm{N}(\sigma_i(\omega_j))^2=\det(\sigma_i(\alpha)\sigma_i(\omega_j)^2=\det(\sigma_i(\alpha\omega_j))^2=d_K(\alpha\omega_1,\ldots,\alpha\omega_n)=\mathrm{N}(\alpha\mathcal{O}_K)^2D(K)$$

Therefore, $|\mathrm{N}(\alpha)|=\left|\prod_{i=1}^n\sigma_i(\alpha)\right|=\mathrm{N}(\alpha\mathcal{O}_K)$. ☐

Lemma 1.3. $\Delta=\mathrm{N}(\mathfrak{b})\cdot|D_K|^{1/2}$.

Proof. Let $\mathfrak{b}$ be generated by $\alpha_1,\ldots,\alpha_n$, so that Γ is generated by $\psi(\alpha_1),\ldots,\psi(\alpha_n)$. Let B be the matrix with enties $\left(\sigma_i(\alpha_j)\right)_{1\leqslant i,j\leqslant n}$. Then $d_K(\mathfrak{b})=d_k(\alpha_1,\ldots,\alpha_n)=\mathrm{N}(\mathfrak{b})^2D_K$. Now consider $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\xrightarrow[\varphi]{\simeq}\mathbb{R}^n$ as $\varphi(x_1,\ldots,x_r,x_{r_1+1}+iy_{r_1+1},\ldots,x_{r_1+r_2}+iy_{r_1+r_2})=(x_1,\ldots,x_r,\sqrt{2}x_{r_1+1},\sqrt{2}y_{r_1+1},\ldots,\sqrt{2}x_{r_1+r_2},\sqrt{2}y_{r_1+r_2})$. Let

$$C=\left(\langle\varphi\circ\psi(\alpha_i),\varphi\circ\psi(\alpha_j)\rangle\right)_{1\leqslant i,j\leqslant n}=\left(\sum_{k=1}^{n}\sigma_k(\alpha_i)\bar{\sigma}_k(\alpha_j)\right)_{1\leqslant i,j\leqslant n}=B^T\bar{B}.$$

Thus $|\det C|^{1/2}=|\det B|$, and $covol(\Gamma)=|\det C|^{1/2}=|d_K(\mathfrak{b})|^{1/2}$, we have $covol(\Gamma)=\mathrm{N}(\mathfrak{b})|D_K|^{1/2}$. ☐

Lemma 1.4. $v = \dfrac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K}$

Proof. Let $\mathcal{F} = \{x \in X : \|x\| \leqslant 1\}$. Define $\mathcal{F}_k = \{x \cdot e^{2\pi k/\omega_K} : x \in \mathcal{F}\}, \quad 0 \leqslant k < \omega_K$. Since multipication by a unit is volume-preserving, $vol(\mathcal{F}_k) = vol(\mathcal{F})$. Define

$$\bar{\mathcal{F}} = \Big(\bigcup_{k=0}^{\omega_K} \mathcal{F}_k\Big) \bigcap \{(x_1, \dots, x_{r_1}, x_{r_1+1}, \dots, x_{r_1+r_2}) : x_1 > 0, \dots, x_{r_1} > 0\}.$$

Multiplying any point in $\bar{\mathcal{F}}$ by $(\pm 1, \dots, \pm 1, 1, \dots, 1)$ shows that $vol(\mathcal{F}) = \frac{2^{r_1}}{\omega_K} vol(\bar{\mathcal{F}})$. And so we will compute $vol(\bar{\mathcal{F}})$ through multiple changes of variables.

Transfor $F : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{R}^n$ as $(x_1, \dots, x_{r_1}, x_{r_1+1}, \dots, x_{r_1+r_2}) \mapsto (\rho_1, \dots, \rho_{r_1}, \rho_{r_1+1}, \varphi_{r_1+1}, \dots, \rho_{r_1+r_2}, \varphi_{r_1+r_2})$, where $\rho_j = |x_j|$, $1 \leqslant j \leqslant r_1 + r_2$ and $\varphi_j = \arg(x_j)$, $r_1 + 1 \leqslant j \leqslant r_1 + r_2$. Thus $x_j = y_j + iz_j = \rho_j e^{i\varphi_j}$, $r_1 + 1 \leqslant j \leqslant r_1 + r_2$. The Jacobian determinant $|J_F| = \rho_{r_1+1} \cdots \rho_{r_1+r_2}$. Then $\bar{\mathcal{F}}$ is given by the conditions $\rho_1 > 0, \dots, \rho_{r_1+r_2} > 0$ and $\prod_{j=1}^{r_1+r_2} \rho_j^{\lambda_i} \leqslant 1$, where $\lambda_i = \begin{cases} 1, & 1 \leq i \leq r_1 \\ 2, & r_1 + 1 \leq i \leq r_1 + r_2. \end{cases}$ And $0 \leqslant \xi_k < 1$ in the formula $\eta(x) = c\lambda + \sum_{i=1}^{r_1+r_2} c_i l(\epsilon)$, $\forall x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, with $\lambda = (\underbrace{1, \dots, 1}_{r_1}, \underbrace{2, \dots, 2}_{r_2})$ and $c = \log \|x\|/n$. It deduces that

$$\log \rho_j^{\lambda_j} = \frac{\lambda_j}{n} \log\Big(\prod_{k=1}^{r_1+r_2} \rho_k^{\lambda_k}\Big) + \sum_{k=1}^{r} \xi_k l_j(\epsilon_k) \quad \text{for each } j\text{'th coordinate of } \eta(x),\ 1 \leqslant j \leqslant r_1 + r_2. \tag{1}$$

These conditions do not restrict φ_j for any value $r_1 + 1 \leqslant j \leqslant r_1 + r_2$. So they take values over $[0, 2\pi)$. Let $\xi = \prod_{j=1}^{r_1+r_2} \rho_j^{\lambda_j}$. Now $\bar{\mathcal{F}}$ is defined by the condition $0 < \xi \leqslant 1$, $0 \leqslant \xi_k < 1$ for $1 \leqslant k \leqslant r_1 + r_2 - 1$. Differentiate the equation (1) we have:

$$\lambda_j \frac{\mathrm{d}\rho_j}{\rho_j} = \frac{\lambda_i}{n} \frac{\mathrm{d}\xi}{\xi} + \sum_{k=1}^{r} l_j(\epsilon_k) \mathrm{d}\xi_k \qquad 1 \leqslant j \leqslant r_1 + r_2.$$

Then

$$\begin{aligned}
|J| &= \begin{vmatrix} \frac{\rho_1}{n \cdot \xi} & \frac{\rho_1}{\lambda_1} l_1(\epsilon_1) & \cdots & \frac{\rho_1}{\lambda_1} l_1(\epsilon_r) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{r_1+r_2}}{n \cdot \xi} & \frac{\rho_{r_1+r_2}}{\lambda_{r_1+r_2}} l_{r_1+r_2}(\epsilon_1) & \cdots & \frac{\rho_{r_1+r_2}}{\lambda_{r_1+r_2}} l_{r_1+r_2}(\epsilon_r) \end{vmatrix} \\
&= \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n \cdot \xi \cdot 2^{r_2}} \begin{vmatrix} \lambda_1 & l_1(\epsilon_1) & \cdots & l_1(\epsilon_r) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{r_1+r_2} & l_{r_1+r_2}(\epsilon_1) & \cdots & l_{r_1+r_2}(\epsilon_r) \end{vmatrix} \\
&= \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n \cdot \xi \cdot 2^{r_2}} \begin{vmatrix} \lambda_1 & l_1(\epsilon_1) & \cdots & l_1(\epsilon_r) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_r & l_r(\epsilon_1) & \cdots & l_r(\epsilon_r) \\ n & 0 & 0 & 0 \end{vmatrix} \\
&= \frac{\rho_1 \cdots \rho_{r_1+r_2}}{\rho_1 \cdots \rho_{r_1} \rho_{r_1+1}^2 \cdots \rho_{r_1+r_2}^2 \cdot 2^{r_2}} \cdot R_K \\
&= \frac{R_K}{2^{r_2} \rho_{r_1+1} \cdots \rho_{r_1+r_2}}
\end{aligned}$$

We now compute the volume of $\bar{\mathcal{F}}$ in $\mathbb{R}^n$. Notice that we have $\varphi : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{R}^n$ as $\varphi(x_1, \dots, x_r, y_{r_1+1} + iz_{r_1+1}, \dots, y_{r_1+r_2} + iz_{r_1+r_2}) = (x_1, \dots, x_r, \sqrt{2}y_{r_1+1}, \sqrt{2}z_{r_1+1}, \dots, \sqrt{2}y_{r_1+r_2}, \sqrt{2}z_{r_1+r_2})$. The Jacobian of this transformation gives $(\sqrt{2})^{2r_2} = 2^{r_2}$. Then:

$$\begin{aligned} vol(\bar{\mathcal{F}}) &= 2^{r_2}\int\cdots\int_{\bar{\mathcal{F}}} \mathrm{d}x_1\cdots\mathrm{d}x_{r_1}y_{r_1+1}\cdots\mathrm{d}z_{r_1+1}\cdots\mathrm{d}y_{r_1+r_2}\mathrm{d}z_{r_1+r_2} \\ &= 2^{r_2}\int\cdots\int_{\bar{\mathcal{F}}} \rho_{r_1+1}\cdots\rho_{r_1+r_2}\mathrm{d}\rho_1\cdots\rho_{r_1+r_2}\mathrm{d}\varphi_{r_1+1}\cdots\varphi_{r_1+r_2} \\ &= 2^{r_2}(2\pi)^{r_2}\int_0^1\cdots\int_0^1 \rho_{r_1+1}\cdots\rho_{r_1+r_2}\,|J|\,\mathrm{d}\xi\mathrm{d}\xi_1\cdots\mathrm{d}\xi_r \\ &= 2^{r_2}(2\pi)^{r_2}\frac{R_K}{2^{r_2}} = (2\pi)^{r_2}R_K \end{aligned}$$

Thus $vol(\mathcal{F}) = \dfrac{2^{r_1}}{\omega_K}vol(\bar{\mathcal{F}}) = \dfrac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K}$ □

Now we complete the whole proof of the weak form of the analytic class number formula:

The proof of Theorem 1.1. Combine Lemma (1.2),(1.3) and (1.4), we have

$$\lim_{s\to 1^+}(s-1)f_A(s) = \mathrm{N}(\mathfrak{b})\frac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K \mathrm{N}}(\mathfrak{b})|D_K|^{1/2} = \frac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K|D_K|^{1/2}}.$$

Summing over each class $A \in \mathcal{C}_K$, we have

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}R_K h_K}{\omega_K|D_K|^{\frac{1}{2}}}$$

□

Keep in mind that the meromorphic continuation of $\zeta_K(s)$ to the whole complex plane is another hard story which is accomplished by Erich Hecke [2] first. Afterwards, Tate established Hecke's theory by harmonic analysis.

1.6 A brief Introduction on Tate's Theory in Weil's Viewpoint

This part is organized in a way following Professor Tian's Notes. For some details we consult to other books, such as Ramakrishnan [3] and Serge Lange [4].

1.6.1 The Local Theorem

Let F be a local field.

Define a Schwartz space $\mathcal{S}(F) = \begin{cases} \left\{\begin{array}{c}\text{Complex-valued locally constant}\\ \text{compactly supported functions on } F\end{array}\right\} & \text{If } F \text{ is } p\text{-adic} \\ \{\text{Schwart functions on } F\} & \text{If } F = \mathbb{R} \text{ or } \mathbb{C}\end{cases}$

Fix a nontrivial additive unitary character $\psi \in \mathrm{Hom}_{\mathrm{cont}}(F,\mathbb{C}^\times)$(i.e., $\mathrm{Im}\psi \neq \{1\}$). For any $\alpha \in F^\times$, let $\psi_\alpha : x \mapsto \psi(\alpha\cdot x)$. Then $\alpha \mapsto \psi_\alpha$ defines a continuous isomorphism $F \xrightarrow{\simeq} \widehat{F} := \mathrm{Hom}_{\mathrm{cont}}(F, S^1)$ as additive topology group.

Let $\mathrm{d}x$ be the self-dual Haar measure on F with respect to ψ. In general, we have Fourier transformation on $\mathcal{S}(F)$: $\widehat{\phi}(x) = \int_F \phi(y)\psi(xy)\mathrm{d}y$, $\forall \phi \in \mathcal{S}(F)$, satisfies that $\widehat{\widehat{\phi}}(0) = \phi(0)$ for all $\phi \in \mathcal{S}(F)$. Let $\chi : F^\times \to \mathbb{C}^\times$ be a character and consider the zeta integral:

$$Z(\phi,\chi,s) = \int_{F^\times}\phi(x)\chi(x)|x|^s\mathrm{d}^\times x, \quad \forall \phi \in \mathcal{S}(F).$$

Let $\mathcal{S}(F)'$ be the space of tempered distributions. For any $\lambda \in \mathcal{S}(F)'$, the Fourier transformation $\widehat{\lambda}$ of λ is defined as $\langle\widehat{\lambda},\phi\rangle = \langle\lambda,\widehat{\phi}\rangle$. $\forall \phi \in \mathcal{S}(F)$. The group $F^\times$ has action ρ on $\mathcal{S}(F)$ and ρ' on $\mathcal{S}(F)'$ in the following ways:

$$\big(\rho(a)\phi\big)(x) = \phi(a\cdot x),\ \langle\rho'(a)\lambda,\phi\rangle = \langle\lambda,\rho(a^{-1})\phi\rangle. \quad \forall a \in F^\times, \phi \in \mathcal{S}(F), \lambda \in \mathcal{S}(F)'.$$

We give the following results without any proof.

Theorem 1.2. *For any character $\chi : F^\times \to \mathbb{C}^\times$, the χ-eigen subspace of $\mathcal{S}(F^\times)$,*

$$\mathcal{S}(F)'^{\chi} := \{\lambda \in \mathcal{S}(F)' : \rho'(a)\lambda = \chi(a)\lambda\}$$

is of one dimension.

Proposition 1.2. $Z_0(\chi) : \phi \mapsto \left.\dfrac{Z(\phi,\chi,s)}{L(\chi,s)}\right|_{s=0}$ *and* $\widehat{Z}_0(\chi) : \phi \mapsto \left.\dfrac{Z(\widehat{\phi},\chi^{-1},1-s)}{L(\chi^{-1},1-s)}\right|_{s=0}$ *both are a basis of the space* $\mathcal{S}(F)'^{\chi}$.

Theorem 1.3. *Let $\chi : F^\times \to \mathbb{C}^\times$ be a character. The zeta integral*

$$Z(\phi,\chi,s) = \int_{F^\times} \phi(x)\chi(x)|x|^s \mathrm{d}^\times x, \quad \forall \phi \in \mathcal{S}(F),$$

is absolutely convergent when $\mathrm{Re}(\chi|\cdot|^s) > 0$ *and has a meromorphic continuation to whole s-plane such that* $\dfrac{Z(\phi,\chi,s)}{L(\chi,s)}$ *is holomorphic, and satisfies the function equation:*

$$\frac{Z(\widehat{\phi},\chi^{-1},1-s)}{L(\chi^{-1},1-s)} = \epsilon(\chi,\psi,s)\frac{Z(\phi,\chi,s)}{L(\chi,s)}.$$

Here $\epsilon(\chi,\psi,s)$ is independent of ϕ and is holomorphic of exponential type.

1.6.2 The Global Theorem

Let K be a number field and its ring of adéles $\mathbb{A}$ is defined to be:

$$\mathbb{A} := \prod_v{}'(K_v,\mathcal{O}_v) = \left\{(a_v) \in \prod_v K_v : a_v \in \mathcal{O}_v \text{ for almost all } v\right\}.$$

Fix a nontrivial additive unitary character $\psi = \otimes_v \psi_v : \mathbb{A}/K \to \mathbb{C}^\times$, let $\mathrm{d}x = \prod_v \mathrm{d}x_v$ be the Haar measure on $\mathbb{A}$ such that $\mathrm{d}x_v$ is self-dual with respect to ϕ_v. The Fourier transformation of a Schwartz function ϕ is defined to be $\widehat{\phi}(y) = \int_{\mathbb{A}} \phi(x)\psi(xy)\mathrm{d}x$. Then $\widehat{\widehat{\phi}}(0) = \phi(0)$. For a Schwartz function $\phi \in \mathcal{S}(\mathbb{A})$, we define the Tate zeta integral

$$Z(\phi,\chi,s) := \int_{\mathbb{A}} \phi(x)\chi(x)|x|^s \mathrm{d}^\times x.$$

We have the similar results compared to the local theory:

Theorem 1.4. *For any Hecke character $\chi : \mathbb{A}^\times/F^\times \to \mathbb{C}^\times$, the χ-eigen subspace of $\mathcal{S}(\mathbb{A})'$,*

$$\mathcal{S}(\mathbb{A})'^{\chi} := \left\{\lambda \in \mathcal{S}(\mathbb{A})' : \rho'(a)\lambda = \chi(a)\lambda\right\}$$

is of one dimension.

Proposition 1.3. $Z_0(\chi) : \phi \mapsto \left.\dfrac{Z(\phi,\chi,s)}{L(\chi,s)}\right|_{s=0}$ *and* $\widehat{Z}_0(\chi) : \phi \mapsto \left.\dfrac{Z(\widehat{\phi},\chi^{-1},1-s)}{L(\chi^{-1},1-s)}\right|_{s=0}$ *both are a basis of the space* $\mathcal{S}(\mathbb{A})'^{\chi}$.

Theorem 1.5. *Let $\chi : \mathbb{A}^\times/K^\times \to \mathbb{C}^\times$ be a Hecke character. The L-series of χ,*

$$L(s,\chi) = \prod_v L(s,\chi_v).$$

is absolutely convergent when $\mathrm{Re}(s) \gg 0$, *has meromorphic continuation and satisfies the function equation:*

$$L(\chi,s) = \epsilon(\chi,s)L(\chi^{-1},1-s),$$

where $\epsilon(s,\chi) = \prod_v \epsilon(\chi_v,\psi_v,s)$ is independent of the choice of ϕ, and is of exponential type.

Theorem 1.6. *Let $\chi : \mathbb{A}^\times/K^\times \to \mathbb{C}^\times$ be a Hecke character. For a Schwartz function $\phi \in \mathcal{S}(\mathbb{A})$, the Tate zeta integral*

$$Z(\phi,\chi,s) \coloneqq \int_{\mathbb{A}} \phi(x)\chi(x)|x|^s \mathrm{d}^\times x$$

is absolutely convergent when $\mathrm{Re}(s) \gg 0$*, has meromorphic continuation to the whole s-plane, and satisfies the function equation $Z(\phi,\chi,s) = Z(\widehat{\phi},\chi^{-1},1-s)$.*

Let $\mathbb{A}^1$ be the subgroup of $\mathbb{A}^\times$ of norm 1 idéles. Take compatible Haar measure for the exact sequences:

$$1 \to \mathbb{A}^1/K^\times \to \mathbb{A}^\times/K^\times \xrightarrow{|\cdot|} K_\infty^+ \to 1$$

By applying Poisson summation formula, we have for any $\phi \in \mathcal{S}(\mathbb{A})$:

$$\begin{aligned} Z(\phi,\chi,s) &= \int_{|x|>1} \phi(x)\chi(x)|x|^s \mathrm{d}^\times x + \int_{|x|<1} \widehat{\phi}(x)\chi^{-1}(x)|x|^{1-s}\mathrm{d}^\times x \\ &+ \delta\cdot \mathrm{Vol}(\mathbb{A}^1/K^\times)\cdot\Big(\frac{\widehat{\phi}(0)}{s-1+\lambda} - \frac{\phi(0)}{s+\lambda}\Big), \end{aligned} \tag{2}$$

where $\delta = 1$ if χ has form $|\cdot|^\lambda$ for some $\lambda \in \mathbb{C}$ and $\delta = 0$ otherwise. It follows from equation (2) that the extended function $Z(\phi,\chi,s)$ is in fact holomorphic everywhere except when $\chi = |\cdot|^\lambda$, in which case it has simple poles at $s = -\lambda$ and $s = 1-\lambda$ with corresponding residues given by $-\mathrm{Vol}(\mathbb{A}^1/K^\times)\phi(0)$ and $\mathrm{Vol}(\mathbb{A}^1/K^\times)\widehat{\phi}(0)$.

We claim that for number field K, $\mathrm{Vol}(\mathbb{A}^1/K^\times) = \dfrac{2^{r_1}(2\pi)^{r_2}h_K R_K}{\omega_K|D_K|^{1/2}}$. Suppose now $\chi = |\cdot|^\lambda$ for some $\lambda \in \mathbb{C}$, and $\widehat{\phi}(0) = 1$. In the case of Dedekind zeta function $\zeta_K(s)$, we show that it has a simple pole at $s = 1$, with residue $\mathrm{Res}_{x=1}\zeta_K(s) = \dfrac{2^{r_1}(2\pi)^{r_2}h_K R_K}{\omega_K|D_K|^{1/2}}$.

2 The Weak Mordell-Weil Theorem

Definition 2.1. An elliptic curve is a pair $(E/K,\mathcal{O})$, where E/K is a smooth curve of genus one and $\mathcal{O}$ is a point in $E(K)$. The distinguished point $\mathcal{O}$ is usually implicit, so we often denote elliptic curves simply with E/K.

Let K be a number field, and E be an elliptic curve defined over K. The set of K-valued points $E(K)$ forms an abelian group. We have the fundamental theorem:

Theorem 2.1 (Mordell-Well)**.** *$E(K)$ is a finitely generated abelian group.*

In this section, we only prove the following theorem.

Theorem 2.2 (Weak Mordell-Weil)**.** *For any positive integer m, the group $E(K)/mE(K)$ is finite.*

The entire proof of the Mordell-Weil theorem involves a theory of heights. From the theory of heights of K-valued points of elliptic curves, it can be seen that if a finite set A of elements of $E(K)$ can be found, such that they generate the group $E(K)$ modulo the subgroup $mE(K)$, then the finite set of elements of $E(K)$ with highest height in A will generate $E(K)$. Thus the problem of computing the rank of the Mordell-Weil group, is reduced to the problem of computing the generators of $E(K)/mE(K)$. The proof given here uses the approach in many materials that can be found online, such as [5], [6] and [7]. Before we get into the main topic, there is a long way to go.

2.1 Elliptic Curves and Maps between Them

2.1.1 The Group Operation

We shall show that elliptic curves can be given a natural group structure. Our first construction of group operation is very intrinsic and relies on the Picard group. We shall see that the Riemann-Roch theorem plays an essential role in this part.

Theorem 2.3 (Riemann-Roch)**.** *Let C/K be a smooth curve of genus g, and let D be a divisor of C atisfying* $\deg D > 2g-2$. *Then* $\ell(D) = \deg D - g + 1$.

Lemma 2.1. Let E/K be a smooth curve of genus one, and let P and Q be points in E. Then the divisors (P) and (Q) are linearly equivalent if and only if $P = Q$.

Proof. One direction is immediate, so start by writing $\operatorname{div} f = (P) - (Q)$ for some $f \in \bar{K}(E)$. Now $f \in \mathcal{L}((Q))$, and since E is smooth of genus one, the RiemannRoch theorem yields $\ell((Q)) = 1$. Because $\mathcal{L}((Q))$ includes K, we see in fact $\mathcal{L}((Q)) = K$. So f is a constant, which implies $\operatorname{div} f = 0$ and consequently $P = Q$. □

Next, recall the definition of $\operatorname{Pic}^0(E)$.

Definition 2.2. Let C/K be a curve. Its divisors of degree zero form a subgroup, which we denote by $\operatorname{Div}^0(C)$. This subgroup contains the principal divisors, and we denote the image of $\operatorname{Div}^0(C)$ under the quotient map $\operatorname{Div}(C) \longrightarrow \operatorname{Pic}(C)$ by $\operatorname{Pic}^0(C)$.

Let E/K be an elliptic curve. Using Lemma 2.1, we now construct a bijection between E and $\operatorname{Pic}^0(E)$ with the intent of inducing a group structure on E from that of $\operatorname{Pic}^0(E)$.

Proposition 2.1. *Let $[D]$ be an element of* $\operatorname{Pic}^0(E)$. *There exists a unique point P in E satisfying $[D] = [(P) - (\mathcal{O})]$, and the map* $\operatorname{Pic}^0(E) \xrightarrow{\sigma} E$ *sending $[D]$ to its corresponding point P is a bijection.*

Proof. As E is smooth of genus one, we see $\ell(D + (\mathcal{O})) = 1$ by Riemann-Roch. Therefore we may choose a nonzero f in $\mathcal{L}(D + (O))$, satisfying $\operatorname{div} f \geqslant -D - (\mathcal{O})$, and the right hand side has $\deg(-D - (O)) = -1$. Yet $\deg \operatorname{div} f = 0$, so we must have $\operatorname{div} f = -D - (\mathcal{O}) + (P)$ for some point P of E. This relation shows D and $(P) - (\mathcal{O})$ are linearly equivalent. We want to show this P is independent of our choice for D. Let D' be any divisor in $\operatorname{Div}^0(E)$. Let P' be a point of E satisfying $[D'] = [(P') - (\mathcal{O})]$. Subtracting this from $[D] = [(P) - (O)]$ yields $[D - D'] = [(P) - (P')]$. Now if $[D] = [D']$, this indicates $[(P)] = [(P')]$ and hence $P = P'$ by Lemma 2.1. Therefore the point P corresponding to $[D]$ is unique, so the map σ is well-defined. The injectivity of *sigma* also follows from this equation, for if $\sigma[D] = P = \sigma[D']$ then $[D - D'] = 0$. Finally, for all points P in E, clearly $[(P) - (\mathcal{O})] = P$, which makes σ surjective as well. □

Remark 2.1. The (algebraic) group operation of $(E/K, \mathcal{O})$ is the group structure induced on E by σ, denoted as $E \times E \xrightarrow{\boxplus} E$ and $E \xrightarrow{\boxminus} E$. The group axioms for E follow from those for $\operatorname{Pic}^0(E)$. We shall give a geometric definition for the group operation in the next part.

2.1.2 Weierstraβ Equations

Fix a field K and an algebraic closure $\bar{K}$. An elliptic curve over $\bar{K}$ is a nonsingular projective curve over $\bar{K}$ of genus 1 with a specified base point. Using algebraic geometry, it can be shown that any such curve can be embedded in $\mathbb{P}^2(\bar{K})$ as the locus of a cubic equation with only one point, the base point, on the line at infinity. Thus any elliptic curve is the solution set of a corresponding Weierstraβ equation.

Definition 2.3. A Weierstraβ equation is an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with coefficients $a_1, \dots, a_6 \in \bar{K}$. Additionally we define the quantities the discriminatn Δ, the j-invariant j, and the invariant differential ω as follows:

$$\begin{aligned}
b_2 &:= a_1^2 + 4a_2, \\
b_4 &:= 2a_4 + a_1a_3, \\
b_6 &:= a_3^2 + 4a_6, \\
b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
c_4 &:= b_2^2 - 24b_4, \\
c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6, \\
\Delta &:= -b_2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\
j &:= c_4^3/\Delta \text{ if } \Delta \neq 0, \\
\omega &:= \frac{\mathrm{d}x}{2y + a_1x + a_3} = \frac{\mathrm{d}y}{3x^2 + 2a_2x + a_4 - a_1y},
\end{aligned}$$

Suppose E/K is an elliptic curve and char$K \neq 2$, then through a change of variables, we may always simplify the Weierstraβ equation to the form

$$E : y^2 = f(x) = 4x^3 + b_2x^2 + 2b^4x + b_6. \tag{3}$$

Then the discriminant Δ of the Weierstraβ equation and the j-invariant of the elliptic curve are given by $\Delta = 16\mathrm{Disc}(f) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$, and $j = \dfrac{b_2^2 - 24b_4}{\Delta}$.

If we further assume char$K \neq 2, 3$, then the Weierestraβ equation may be further simplified to the form

$$E : y^2 = f(x) = x^3 + Ax + B \tag{4}$$

Proposition 2.2. *Let E and E' be two elliptic curves defined over $\bar{K}$.*

(a) *Say E/K is defined over K and is given by the Weierstraβ equation in Equation (3). Then*

  (i) *E is nonsingular if and only if $\Delta \neq 0$,*

  (ii) *E has a node if and only if $\Delta = 0, b_2^2 - 24b_4 \neq 0$,*

  (iii) *E has a cusp if and only if $\Delta = 0, b_2^2 - 24b_4 = 0$*

(b) *The two elliptic curves E and E' are isomorphic if and only if $j(E) = j(E')$.*

(c) *Take any $j_0 \in \bar{K}$. Then there is an elliptic curve $E''/K(j_0)$ with $j(E'') = j_0$.*

Proof. See [8, III.3]. □

Now we assert that Weierstraβ equations provide a more concrete approach to elliptic curves.

Theorem 2.4. *Let $(E/K, \mathcal{O})$ be an elliptic curve.*

(a) *There exist x and y in $K(E)$ such that the map $E \xrightarrow{\phi} \mathbb{P}^2$ defined by $\phi(P) = [x : y : 1]$ is an isomorphism from E to a Weierstraβ equation with coefficients in K and ϕ maps $\mathcal{O}$ to $[0:1:0]$.*

(b) *Let E_1/K and E_2/K be two Weierstraβ equations for E satisfying the properties enumerated in (a). Then E_1 and E_2 are isomorphic by a change of variables in the form*

$$X_2 = u^2X_1 + r \qquad Y_2 = u^3Y_1 + su^2X_1 + t \qquad \text{for some } u \in K^\times \text{ and } r, s, t \in K.$$

(c) *Conversely, by choosing a distinguished point $\mathcal{O}$, every smooth Weierstraβ equation E/K is an elliptic curve $(E/K, \mathcal{O})$.*

Proof. See [8, Proposition III.3.3] □

Definition 2.4. Let C/K be a smooth curve, and let P and Q be points on C. The secant line on C defined by P and Q is the smooth curve L in $\mathbb{P}^2$ given as follows. If $P \neq Q$, let L be the unique line going through P and Q, otherwise, let L be the line tangent to C at $P = Q$.

Definition 2.5. Let E/K be an elliptic curve. Let P and Q be points on E, and let L be the secant line on E defined by P and Q. Since Weierstraβ equations are given by cubics, Bezouts theorem shows $E \cap L = \{P, Q, R\}$ as a multiset. Next, let L' be the secant line on E defined by $\mathcal{O}$ and R. Applying Bezout again indicates $E \cap L' = \{O, R, S\}$ as a multiset. Finally, let L'' be the secant line on E defined by O and P. As usual $E \cap L'' = \{O, P, T\}$ by Bezouts theorem.

The (geometric) group operation is given by the binary operation $E \times E \xrightarrow{\oplus} E$ as $(P, Q) \mapsto S$ and the inverse map $E \xrightarrow{\ominus} E$ as $P \mapsto T$.

See Figure 1 for an example, in which $(0, 2)$ and $(1, 0)$ add to $(3, 4)$ in the group law (the figure presented here cites the material [7, Section 11.1]). In fact the algebraic group operation matches with the geometric group operation.

Proposition 2.3. *Let E/K be an elliptic curve. The algebraic group operation $E \times E \xrightarrow{\boxplus} E$ and geometric group operation $E \times E \xrightarrow{\oplus} E$ are the same map, as are $E \xrightarrow{\boxminus} E$ and $E \xrightarrow{\ominus} E$.*

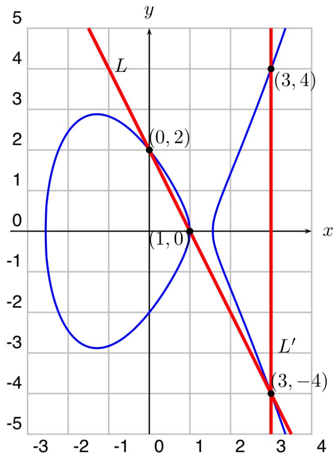

Figure 1: The Group Law:$(1,0) + (0,2) = (3,4)$ on $y^2 = x^3 - 5x + 4$

Proof. In the situation of Definition 2.5, let $g(X,Y,Z)$ and $g'(X,Y,Z)$ be the homogeneous linear equations defining L and L', respectively. More explicitly, $L \cap E = \{P,Q,R\}$ and $L' \cap E = \{O,R,S\}$ Let $f = g/g' \in K(E)$. Then $(f) = P+Q+R-\mathcal{O}-R-S = P+Q-\mathcal{O}-S \Rightarrow S$ are linearly equivalent to $P+Q-\mathcal{O}$. Therefore $\boxplus(P,Q) = \oplus(P,Q)$ and for the same reason $\boxminus P = \ominus P$. □

Proposition 2.3 enables us to interchangeably use the algebraic and geometric definitions for the group operation, which we will simply denote by $E \times E \xrightarrow{+} E$ and $E \xrightarrow{-} E$. The geometric description of addition in E allows explicit calculations with polynomial equationssee Group Law Algorithm III.2.3 in [8]. As a corollary, we see elliptic curves are abelian varieties

Corollary 2.1. *Let E/K be an elliptic curve. Then the addition and negation maps $E \times E \xrightarrow{+} E$ and $E \xrightarrow{-} E$ are morphisms defined over K.*

This in turn shows the K-valued points of an elliptic curve form a subgroup, denoted by $E(K)$.

Corollary 2.2. *Let E/K be an elliptic curve. Then $E(K)$ is a subgroup of E.*

Proof. The identity $\mathcal{O}$ is in $E(K)$, and $E(K)$ is closed under addition since $E \times E \xrightarrow{+} E$ is a morphism defined over K. □

2.1.3 Maps between Elliptic Curves

We have seen that elliptic curves are abelian varieties, that is, projective varieties and abelian groups in a compatible way. From a view of category theory, we also expect morphisms of elliptic curves to have abelian group and ring structures similar to those of abelian group homomorphisms.

Definition 2.6. Let $(E_1/K, \mathcal{O}_1)$ and $(E_2/K, \mathcal{O}_2)$ be elliptic curves. An isogeny from E_1 to E_2 is a morphism $E_1 \xrightarrow{\phi} E_2$ that sends $\phi(\mathcal{O}_1) = \mathcal{O}_2$. If ϕ is constant, it must be valued on $\mathcal{O}_2$. We call this the zero isogeny and denote it by $\phi = [0]$.

If ϕ is not the zero isogeny, it is a non-constant morphism of smooth curves, which makes it finite and surjective. Therefore we may consider the degree $\deg\phi$. For the zero isogeny, we set $\deg[0] = 0$.

Proposition 2.4. *Let $E_1 \xrightarrow{\phi} E_2$ be an isogeny. Then ϕ is a group homomorphism.*

Proof. Of course $[0]$ is the trivial homomorphism, so suppose ϕ is non-constant. Here ϕ induces a homomorphism $\mathrm{Pic}^0(E_1) \xrightarrow{\phi} \mathrm{Pic}^0(E_2)$, and since ϕ sends $\mathcal{O}_1$ to $\mathcal{O}_2$. Therefore ϕ is also a group homomorphism since we have the commutative diagram below.

$$\begin{tikzcd}
\mathrm{Pic}^0(E_1) \arrow[r, "\sigma_1"] \arrow[d, "\phi_*"'] & E_1 \arrow[d, "\phi"'] \\
\mathrm{Pic}^0(E_2) \arrow[r, "\sigma_2"] & E_2
\end{tikzcd}$$

□

Definition 2.7. Let E_1/K and E_2/K be elliptic curves. We write $\mathrm{Hom}(E_1, E_2)$ for the set of isogenies $E_1 \xrightarrow{\phi} E_2$. From here, we form the special hom-sets $\mathrm{End}(E_1)$ and $\mathrm{Aut}(E_1)$ as usual.

Theorem 2.5. *Let E_1/K and E_2/K be elliptic curves.*

(a) *The abelian group $\mathrm{Hom}(E_1, E_2)$ is torsion-free.*

(b) *The ring $\mathrm{End}(E_1)$ has no zerodivisors. In particular, it has characteristic 0.*

Proof. See [8, Proposition III.4.2] □

Let E/K be an elliptic curve. Extending our terminology for the zero isogeny, for any integer m we denote the image of m under the unique ring homomorphism $\mathbb{Z} \longrightarrow \mathrm{End}(E)$ by $[m]$. Theorem 2.5 shows this homomorphism is injective, so for nonzero m the morphism $[m]$ is a finite map. This makes the m-torsion subgroup of E finite. Moreover we give the following results directly.

Proposition 2.5. *Let E/K be an elliptic curve, and let m be a positive integer. If $\mathrm{Char}K \nmid m$, then $E[m]$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as abstract groups.*

Proof. See [8, Chapter III]. □

2.2 Reduction of elliptic curves

Let K_v be a local field, complete with repect to a discrete valuation v with ring of integers $\mathcal{O}_v = \{x \in K : v(x) \geqslant 0\}$, maximal ideal $\mathfrak{m}_v$, uniformizer ϖ (i.e., $\mathfrak{m}_v = \varpi\mathcal{O}_v$), and residue field $k_v = \mathcal{O}_v/\mathfrak{m}_v$ with characteristic p. We denote reduction modulo $\mathfrak{m}$ by a tilde.

There is a reduciton of the projective plane: $\mathbb{P}^2(K) \xrightarrow{\pi} \mathbb{P}^2(k)$ which is defined as follows. Take some $[a : b : c] \in \mathbb{P}^2(K)$. By multiplying by some element of R such that $a, b, c \in R$. Then dividing by an appropriate power of ϖ, we may assume

$$\min\{v(a), v(b), v(c)\} = 0 \tag{5}$$

Then use the natural reduction of $R \xrightarrow{\pi} R/\mathfrak{m} = k$, we have $[\widetilde{a : b : c}] = [\tilde{a} : \tilde{b} : \tilde{c}]$ is well-defined since the situation $\tilde{a} = \tilde{b} = \tilde{c} = 0$ is impossible by equation (5).

Let E/K be an elliptic curve over K and assume E is the solution set to a Weierstraβ equation $f(X, Y, Z) = 0$ with discriminant Δ. Via the reduction $\tilde{f}(X, Y, Z) = \tilde{0}$ defineds another curve $\tilde{E}/k$ over k with discriminant $\tilde{\Delta}$. Then $\tilde{E}$ is an elliptic curve as long as $\tilde{\Delta} \neq \tilde{0}$ (as long as $\Delta \notin \mathfrak{m}$). In this case, there is a natural reduction map of elliptic curves $\pi : E/K \to \tilde{E}/k$ given by the projection space reduction defined above. However, there could be many Weierstraβ equations for E/K_v, so one must discern which ones reflect the essential properties of E/K_v after reducing modulo $\mathfrak{m}_v$.

Definition 2.8. Let E/K_v be an elliptic curve, and let $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ be a Weierstraβ equation for E. If all the a_i lie in $\mathcal{O}v$ and $v(\Delta)$ is minimal while upholding this condition, we say this is a minimal equation for E.

Proposition 2.6. *Let E/K_v be an elliptic curve. Then E has a minimal equation.*

Proof. Let $Y^2+a_1XY+a_3Y = X^3+a_2X^2+a_4X+a_6$ be a Weierstraβ equation for E/K_v. Direct calculation indicates the substitution $(X, Y) \mapsto (u^{-2}X, u^{-3}Y)$ yields another Weierstraβ equation for E/K_v with a_i replaced by u^ia_i, so taking $u = \pi^N$ for sufficiently large N yields a Weierstraβ equation with coefficients in $\mathcal{O}_v$. Now note that since $v(\Delta)$ is a polynomial in the a_i, so Δ is in $\mathcal{O}_v$ if the a_i are. Thus $v(\Delta)$ is non-negative, and we may apply well-ordering to show minimal equations exist. □

Minimal equations are precisely the Weierstraβ equations that preserve nice properties when reduced modulo $\mathfrak{m}_v$. Before elaborating, we clarify which of the changes of variables outlined in Proposition 2.4 preserve minimality.

Proposition 2.7. *Let E/K_v be an elliptic curve.*

(a) *A minimal equation is unique up to change of coordinates in the form*

$$X = u^2X' + r \qquad Y = u^3Y' + su^2X' + t \qquad \text{for some } u \in \mathcal{O}_v^\times \text{ and } r, s, t \in \mathcal{O}_v.$$

(b) *As a converse, any substitution used to obtain a minimal equation from a Weierstraβ equation with coefficients in* $\mathcal{O}_v^\times$ *is in above form, except the restriction on* u *is related to* $u \in \mathcal{O}_v$.

Proof. See [8, Proposition VII.1.3]. □

Now we use minimal equations to define elliptic curves reduced modulo $\mathfrak{m}_v$.

Definition 2.9. Let E/K_v be an elliptic curve. We denote the Weierstraβ equation obtained from reducing a minimal equation for E modulo $\mathfrak{m}_v$ by $\tilde{E}/k_v$.

Remark 2.2. This $\tilde{E}/k_v$ is not necessarily smooth, so it may not define an elliptic curve over k_v. We will restrict to the $\tilde{E}/k_v$ smooth case. For reference, see [8, Chapter VII].

At the first place we have an exact sequence $0 \to \mathfrak{m}_v \to \mathcal{O}_v \to k_v \to 0$, we obtain a similar short exact sequence of elliptic curves.

Theorem 2.6. *Let* E/K_v *be an elliptic curve such that* $\tilde{E}/k_v$ *is smooth.*

(a) *Then the reduction modulo* $\mathfrak{m}_v$ *map induces a surjective group homomorphism* $E(K_v) \xrightarrow{\pi} \tilde{E}/k_v$.

(b) *The kernel* Kerπ *is independent of the minimal equation chosen for defining* $\tilde{E}/k_v$. *We denote it by* $E_1(K_v)$. *Altogether we obtain a short exact sequence*

$$0 \to E_1(K_v) \to E(K_v) \to \tilde{E}/k_v \to 0.$$

Proof. See [8, Proposition VII.2.1]. □

2.2.1 Elliptic Curve Formal Groups

Since K_v is a complete non-Archimedean local field, they manifest as formal power series expansions of group operations. Let us take a brief look into formal groups.

Definition 2.10. Let A be a commutative ring. A formal group over A is a power series $F(X, Y)$ in two variables with coefficients in A satisfying

(i) $F(X, 0) = X$ and $F(0, Y) = Y$.

(ii) There exists a unique power series $i(T)$ in one variable with coefficients in A satisfying $F(T, i(T)) = 0$.

(iii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

(iv) $F(X, Y) = F(Y, X)$.

(v) $F(X, Y) = X + Y \bmod (X^2, XY, Y^2)$.

We denote formal groups by F/A.

Example 4. Let E/K_v be an elliptic curve. We aim to construct a formal group over K_v corresponding to elliptic curve addition. Since power series expansions happen best around the origin and the identity element, we first make a change of variables that sends $\mathcal{O}$ to $(0, 0)$. More specifically, we set $Z = -X/Y$ and $W = -1/Y$, transforming the defining Weierstraβ equation to

$$W = z^3 + a_1ZW + a_2Z^2W + a_3W^2 + a_4ZW^2 + a_6W^3.$$

Notice this is a polynomial expression for W in terms of W and Z. By inductively substituting the right hand side, we obtain a formal power series of W in Z. Thus we may use Z to parametrize our formal group.

By using explicit polynomial formulas for the elliptic curve group operation, we can construct two formal power series $F(Z_1, Z_2)$ and $i(Z)$ that correspond to the elliptic curve group operations. For detailed calculations of this procedure, see [8, Chapter IV.1].

Let A be a commutative ring. The collection of formal groups over A forms a category once we define appropriate morphisms.

Definition 2.11. Let F/A and G/A be formal groups. A homomorphism from F to G over A is a power series $f(T)$ in one variable with coefficients in A such that $f(F(X,Y)) = G(f(X), f(Y))$.

Example 5. Let F/A be a formal group, and let m be an integer. We can inductively define a power series $f_m(T)$ by setting

$$f_0(T) = 0 \qquad f_{m+1}(T) = F(f_m(T), T) \qquad f_{m-1} = F(f_m(T), i(T)).$$

These f_m are formal group endomorphisms of F/A. They are analogous to multiplication by m endomorphisms of abelian groups. In fact, if m is a unit in A, then f_m is a formal group isomorphism. See [8, Proposition IV.2.3].

Definition 2.12. Let E/K_v be an elliptic curve, and let F/K_v be its corresponding formal group law as described in Example 4 . Then the group associated to F/K_v, denoted by $\widehat{E}(\mathfrak{m}_v)$, is the group given as follows. The underlying set of $\widehat{E}(\mathfrak{m}_v)$ is $\mathfrak{m}_v$, the binary operation $\mathfrak{m}_v \times \mathfrak{m}_v \to \mathfrak{m}_v$ maps (z_1, z_2) to $F(z_1, z_2)$, and the inverse map $\mathfrak{m}_v \to \mathfrak{m}_v$ takes z to $i(z)$.

Proposition 2.8. *Let E/K_v be an elliptic curve given by a minimal equation, and let $\widehat{E}(\mathfrak{m}_v)$ be the group described above. Then $E_1(K_v)$ and $\widehat{E}(\mathfrak{m}_v)$ are isomorphic via the map*

$$\widehat{E}(\mathfrak{m}_v) \longrightarrow E_1(K_v) \qquad \textit{that sends} \quad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right).$$

Proof. See [8, Proposition VII.2.2]. □

Lemma 2.2. Let E/K_v be an elliptic curve, and let $\widehat{E}(\mathfrak{m}_v)$ be the group given defined above. Let $p = \operatorname{Char} k_v$. Then every torsion element in $\widehat{E}(\mathfrak{m}_v)$ has order a power of p.

Proof. We only have to prove that there are no nontrivial torsion elements with order relatively prime to p. Let m be a positive integer prime to p. Then m is not in $\mathfrak{m}_v$, so it is a unit in $\mathcal{O}_v$. Now multiplication by m is precisely the group endomorphism induced by f_m from Example 5, and because f_m was a formal group isomorphism, multiplication by m is an actual group isomorphism. Thus it has trivial kernel, making $\widehat{E}(\mathfrak{m}_v)[m] = 0$. □

Theorem 2.7. *Let E/K_v be an elliptic curve, let m be a positive integer not divisible by $p = \operatorname{Char} k_v$, and suppose $\tilde{E}/k_v$ is smooth. Then the reduction map $E(K_v)[m] \xrightarrow{\pi} \tilde{E}(k_v)[m]$ on m-torsion is injective.*

Proof. Since Proposition 2.8 and Lemma 2.2 indicate $E_1(K_v)$ has no nontrivial m-torsion, the m-torsion of $E(K_v)$ trivially intersects $E_1(K_v)$. From here, the short exact sequence provided in Theorem 2.6 indicates the m-torsion of $E(K_v)$ embeds into $\tilde{E}(k_v)[m]$. □

2.3 Galois Cohomology and Kummer Theory

Over an algebraic closure $\bar{K}$ of K, the multiplication map $m : E(\bar{K}) \to E(\bar{E})$ is surjective. However over a number field K, the solutions to an equation of the form $mQ = P$, for some $P \in E(K)$, lies in $E(\bar{K})$. The essence is to control the field extensions of K generated by Q as P varies over the K-valued points of E. A convenient way to do this is via Galois cohomology.

Let G be a group, and M be a G-module, i.e, an abelian group M with an action of $G : M \times G \to M$, denoted by $(x, \sigma) \mapsto x^\sigma$. From homological algebra(Here we consult to a nice note written by Zheng Weizhe [9]), we have the cohomology groups $H^i(G, M)$ for $i \geqslant 0$, satisfying:

(i) Given a short exact sequence of G-modules:

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

there is an associated long exact sequence of cohomology groups:

$$\cdots \to \mathrm{H}^{i-1}(G, M'') \to \mathrm{H}^i(G, M') \to \mathrm{H}^i(G, M) \to \mathrm{H}^i(G, M'') \to \cdots$$

(ii) The 0'th cohomology group is $\mathrm{H}^0(G,M)=\{x\in M : x^\sigma = x \text{ for all } \sigma\in G\}=G^M$.

(iii) Explicitly, $\mathrm{H}^1(G,M)$ can be described as follows: Let $\mathrm{Z}^1(G,M)=\{\xi : G\to M : \xi(\sigma\tau)=\xi(\sigma)^\tau+\xi(\tau),\ \forall\sigma,\tau\in G\}$, be the groups of cocycles. $\mathrm{B}^1(G,M)=\{\xi : G\to M : \xi(\sigma)=g^\sigma-g, \text{ for some } g\in G\}$, be the group of coboundaries. Then $\mathrm{H}^1(G,M)=\mathrm{Z}^1(G,M)/\mathrm{B}^1(G,M)$.

For example, if G acts trivially on M, then $\mathrm{H}^1(G,M)=\mathrm{Hom}(G,M)$.

The absolute Galois group of K is defined as:

$$G_K := \varprojlim_{L|K} \mathrm{Gal}(L|K),$$

given as a projective limit of the finite Galois groups $\mathrm{Gal}(L|K)$, where L runs over all finite Galois extensions of K. If L is a finite Galois extension of K with Galois group $\mathrm{Gal}(L|K)$ we can treat any $\mathrm{Gal}(L|K)$ module M_L as a G_K module. More genrally, $M=\cup_L M_L$, where M_L is a $\mathrm{Gal}(L|K)$-module and L runs over all finite *Galois* extensions of K contained in $\bar{K}$ and the actions of $\mathrm{Gal}(L|K)$ are compatible, then such M is called a G_K-module. Since taking cohomology is a contravariant functor, for such an M we define the Galois cohomology groups:

$$\mathrm{H}^i(G,M) := \varinjlim_{L|K} \mathrm{H}^i(\mathrm{Gal}(L|K), M_L),$$

where L runs over all finite Galois extensions of K.

Theorem 2.8 (Hilbert 90)**.** *Consider a Galois extension $L|K$ with corresponding Galois group G. We have* $\mathrm{H}^1(G,L^\times)=\mathrm{H}^1(G,L)=0$.

Suppose K is a number field and fix a positive integer m. Let G_K denote the absolute Galois group $\mathrm{Gal}(\bar{K}|K)$. Consider the exact sequence:

$$1\to\mu_m\to\bar{K}^\times\xrightarrow{m}\bar{K}^\times\to 1.$$

The long exact sequence is:

$$1\to\mu_m(K)\to K^\times\xrightarrow{m}K^\times\to\mathrm{H}^1(G_K,\mu_m)\to\mathrm{H}^1(G_K,\bar{K}^\times)=0,$$

where $\mathrm{H}^1(G_K,\bar{K}^\times)=0$ by Theorem 2.8.

Assume now that the group μ_m of m'th roots of unity is contained in K. Using Galois cohomology we obtain a relatively simple classification of all abelian extensions of K with Galois group cyclic of order dividing m. Since the action of G_K on μ_m is trivial, by our hypothesis that $\mu_m\subseteq K$, we see that $\mathrm{H}^1(G_K,\mu_m)=\mathrm{Hom}(G_K,\mu_m)$. Thus we obtain an exact sequence:

$$1\to\mu_m\to K^\times\xrightarrow{m}K^\times\xrightarrow{\delta}\mathrm{Hom}(G_K,\mu_m)\to 1,$$

or equivalently, $K^\times/(K^\times)^m\cong\mathrm{Hom}(G_K,\mu_m)$ with explicit isomorphism

$$\begin{array}{rcl} K^\times/(K^\times)^m & \xrightarrow{\delta} & \mathrm{Hom}(G_K,\mu_m) \\ a & \mapsto & \left[\sigma\mapsto\dfrac{(\sqrt[m]{a})^\sigma}{\sqrt[m]{a}}\right] \end{array}$$

δ is known as Kummer map. By Galois theory, homomorphisms $\mathrm{Gal}(\bar{K}^\times|K)\to\mu_m$ correspond to cyclic abelian extensions of K with Galois group a subgroup of the cyclic group μ_m of order m. Through the isomorphism δ, we know that every such extension is of the form $K(\sqrt[m]{a})$ for some $a\in K$.

Moreover, let $K^{(m)}$ denote the maximal m-exponent extension of K inside $\bar{K}$(by m-exponent extension we mean that the corresponding Galois group is m-exponent). Then Kummer theory shows that there is a $1:1$ correspondence between the following two sets:

$$\begin{array}{rcl} \{\Sigma\subseteq K^\times/(K^\times)^m \text{ subgroup}\} & \xleftrightarrow{1:1} & \{\text{subextension of } K^{(m)}|K\} \\ \Sigma & \mapsto & K^\Sigma := K(\sqrt[m]{a},\, a\in\Sigma) \\ (L^\times)^m\cap K^\times & \leftarrow\!\shortmid & L|K : K\subseteq L\subseteq\bar{K} \end{array}$$

Proposition 2.9. *Let K be a number field, $a \in K^\times$ and $\mathfrak{p} \nmid m$ prime of K. Then $K(a^{1/m})$ over K is unramified at $\mathfrak{p}$ if and only if $m | \mathrm{ord}_\mathfrak{p}(a)$.*

Theorem 2.9. *Let K be a number field and assume $\mu_m \subseteq K$, where m is a positive integer. Let S be a finite set of primes os K containing all primes dividing m. Let L be the maximal m-exponent abelian extension over K contained in $\bar{K}$ unramified outside S, then $[L:K] < \infty$.*

Proof. First we have the exact sequence:

$$1 \to \mathcal{O}_K^\times / \mathcal{O}_K^{\times m} \to \{a \in K^\times / K^{\times m} : (a) = \mathfrak{a}^m \text{ for some } \mathfrak{a} \text{ fractional ideal}\} \to \mathrm{Cl}_K[m] \to 1$$

second, we define a ring:

$$\mathcal{O}_{K,S} := \{a \in K^\times : \mathrm{ord}_\mathfrak{p}(a\mathcal{O}_K) \geqslant 0 \text{ all } \mathfrak{p} \notin S\} \cup \{0\}.$$

Notice that $\mathcal{O}_{K,S}$ is just the localization of $\mathcal{O}_K$ by a multiplicative set $\bigcap_{\mathfrak{p} \notin S}(\mathcal{O}_K - \mathfrak{p})$, thus also a Dedekind domain. Let $K(S,m) = \{a \in K^\times / K^\times : m | \mathrm{ord}_\mathfrak{p}(a) \text{ for all } \mathfrak{p} \notin S\}$ be a supgroup of $K^\times / K^{\times m}$. A little analysis shows that $K(S,m) = \{a \in K^\times / K^{\times m} : a\mathcal{O}_{K,S} = \mathfrak{a}^m$ for some $\mathfrak{a}$ fractional ideal of $\mathcal{O}_{K,S}\}$. Now similarly consider the following exact sequence:

$$1 \to \mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times m} \to K(S,m) \to \mathrm{Cl}_K[m] / \langle [\mathfrak{p}], \mathfrak{p} \in S \rangle \to 1$$

We claim that $\mathcal{O}_{K,S}^\times$ is a finitely generated abelian group of rank $r_1 + r_2 - 1 + \#S$. Indeed, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes in S. Define a map $\phi : \mathcal{O}_{K,S}^\times \to \mathbb{Z}^n$ by $\phi(u) = (\mathrm{ord}_{\mathfrak{p}_1}(u), \ldots, \mathrm{ord}_{\mathfrak{p}_n}(u))$. We have an exact sequence:

$$1 \to \mathcal{O}_K^\times \to \mathcal{O}_{K,S}^\times \xrightarrow{\phi} \mathbb{Z}^n.$$

Let h be the class number of $\mathcal{O}_K$. For each i there exists $\alpha_i \in \mathcal{O}_K$ such that $\mathfrak{p}_i^h = (\alpha_i)$. But $\alpha_i \in \mathcal{O}_{K,S}^\times$ since $\mathrm{ord}_\mathfrak{p}(\alpha_i) = 0$ for all $\mathfrak{p} \notin S$ (by unique factorization). Then $\phi(\alpha_i) = (0, \ldots, 0, h, 0, \ldots, 0)$. It follows that $(h\mathbb{Z})^n \subseteq \mathrm{Im}(\phi)$, so the image has finite index in $\mathbb{Z}^n$. It follows that $\mathcal{O}_{K,S}^\times$ has rank equal to $r_1 + r_2 - 1 + \#S$. Therefore $K(S,m)$ is a finite subgroup of $K^\times / K^{\times m}$ by the exact sequence. Now if L is an m-exponent abelian extension of K unramified outside S, L is generated by all m'th roots of the elements of $K(S,m)$ by Proposition 2.9, thus finite degree. □

2.4 Ramification Theory of Galois Extensions

Let K be a number field and denote $\mathcal{O}_K$ to be A. The residue field k of K with respect to $\mathfrak{p}$ is the residue field of $A_\mathfrak{p}$. The completion of K with repsect to $\mathfrak{p}$ is the field of fractions of the completion of $A_\mathfrak{p}$ with respect to the unique maximal ideal $\mathfrak{p}$ and is denoted as $K_\mathfrak{p}$.

Proposition 2.10. *Let $L|K$ be a finite Galois extension and $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. Then* $\mathrm{Gal}(L|K)$ *acts transitively on S, the set of primes $\mathfrak{q} \subseteq \mathcal{O}_L$ above $\mathfrak{p}$.*

Definition 2.13. Using the setup from Proposition (2.10), for $\mathfrak{q} \in S$, the decomposition group of $\mathfrak{q}$ is

$$D_\mathfrak{q}(L|K) = \mathit{Stab}(\mathfrak{q}) \leqslant \mathrm{Gal}(L|K).$$

Proposition 2.11. *$D_\mathfrak{q}(L|K)$ is precisely the Galois group of the corresponding extension of completions. That is,*

$$\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) = D_\mathfrak{q}(L|K)$$

Proposition 2.12. *With the same setup as above, let k(resp. l) be the residue field of K (resp. L) with respect to $\mathfrak{p}$ (resp. $\mathfrak{q}$). Via passage to the quotient, the map $\epsilon : D_\mathfrak{q}(L|K) \to \mathrm{Gal}(l|k)$ is a surjection.*

The inertia subgroup of $\mathfrak{q}$ is defined as $\mathrm{I}_\mathfrak{q}(L|K) = \ker(\epsilon)$.

Theorem 2.10. *Using the previous setup, let $G = \mathrm{Gal}(L|K)$, $D = D_\mathfrak{q}(L|K)$, and $I = I_\mathfrak{q}(L|K)$. We have the following picture. Here the columns are field extensions. The Galois group of an extension from the first row to the fourth row is G, second to fourth is D, third to fourth is I, second to third is D/I. The third to fourth row extensions are totally ramified at $\mathfrak{q}$ and all extensions below the fourth row are unramified at $\mathfrak{q}$.*

$$\begin{tikzcd}
\mathfrak{q} & \subset & O_L & \subset & L \arrow[r, dash] \arrow[d, dash, "I"] \arrow[dd, dash, bend right, "D"'] \arrow[ddd, dash, bend right=60, "G"'] & L_{\mathfrak{q}} \arrow[d, dash, "I"] \arrow[dr, dash] & \\
 & & & & L^I \arrow[r, dash] \arrow[d, dash] & L^I_{\mathfrak{q}} \arrow[r, dash] \arrow[d, dash] & l \arrow[d, dash, "D/I"] \\
 & & & & L^D \arrow[r, dash] \arrow[d, dash] & K_{\mathfrak{p}} \arrow[r, dash] \arrow[dl, dash] & k \\
\mathfrak{p} & \subset & O_K & \subset & K & &
\end{tikzcd}$$

2.5 Proof of the Weak Mordell-Weil Theorem

We begin with a lemma.

Lemma 2.3. Suppose $L|K$ is a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is finite.

Proof. Consider a short exact sequence of $G_L = \mathrm{Gal}(L|K)$-modules:

$$0 \to E(L)[m] \to E(L) \xrightarrow{m} mE(L) \to 0.$$

Through Galois cohomology, this induces the long exact sequence:

$$0 \to E(K)[m] \to E(K) \xrightarrow{m} E(K) \cap mE(L) \xrightarrow{\delta} \mathrm{H}^1(G_L, E(L)[m]) \to \cdots$$

and in particular $H \hookrightarrow \mathrm{H}^1(G_L, E(L)[m])$, where $H = \dfrac{E(K) \cap mE(L)}{mE(K)}$. However, G_L and $E(L)[m]$ are finite so $\mathrm{H}^1(G_L, E(L)[m])$ is finite so H is finite. Then it follows from the exact sequence:

$$0 \to H \to E(K)/mE(K) \to E(L)/mE(L)$$

that $E(K)/mE(K)$ is finite. □

Remark 2.3. From this lemma, by taking L to be the Galois closure of the finite extension $K(E[n])/K$, it suffices to prove the weak Mordell-Weil theorem under the assumption $E[n] \subseteq E(K)$.

Suppose E is an elliptic curve over a number field K, and fix a positive integer m. Just as with number fields, we have an exact sequence:

$$0 \to E[m] \to E \xrightarrow{m} E \to 0.$$

The long exact sequence is:

$$0 \to E[m](K) \to E(K) \xrightarrow{m} E(K) \to \mathrm{H}^1(G_K, E[m]) \to \mathrm{H}^1(G_K, E)[m] \to 0.$$

From this we obtain a short exact sequence:

$$0 \to E(K)/mE(K) \to \mathrm{H}^1(G_K, E[m]) \to \mathrm{H}^1(G_K, E)[m] \to 0.$$

By assumption we have that $E[m] \subseteq E(K)$, i.e., all m-torsion points are defined over K. Then $\mathrm{H}^1(G_K, E[m]) = \mathrm{Hom}(G_k, (\mathbb{Z}/m\mathbb{Z})^2)$, and the sequence induces an inclusion with explicit homomorphism:

$$\begin{array}{rcl} E(K)/mE(K) & \hookrightarrow & \mathrm{Hom}(G_K, (\mathbb{Z}/m\mathbb{Z})^2) \\ P & \mapsto & \left[\sigma \mapsto \left(\dfrac{P}{m}\right)^{\sigma} - \dfrac{P}{m}\right] \end{array}$$

Given a point $P \in E(K)$, we obtain a homomorphism $\varphi : G_K \to (\mathbb{Z}/m\mathbb{Z})^2$, whose kernel defines an abelian extension $L|K$ that has m-exponent (i.e., subextension of $K^{(m)}$ which is the maximal abelian extension of K that has m-exponent). The amazing fact is that L can be ramified at most at the primes of bad reduction for E and the primes that divide m. Thus we can apply Theorem 2.9 to show that L is of finite degree.

Theorem 2.11. *If $P \in E(K)$ is a point, then the field L obtained by adjoining to K all coordinates of all choices of $Q = \frac{1}{m}P$ is unramified outside m and the primes of bad reduction for E.*

Proof. By Theorem 2.7, we have the natural reduction map $\pi : E(K)[m] \to \tilde{E}(\mathcal{O}_K/\mathfrak{p})$ is injective. As above, $\sigma(Q) - Q \in E(K)[m]$ for all $\sigma \in \mathrm{Gal}(\bar{K}|K)$. Let $I_\mathfrak{p} \subseteq \mathrm{Gal}(L|K)$ be the inertia group at $\mathfrak{p}$. Then by definition of interia group. $I_\mathfrak{p}$ acts trivially on $\tilde{E}(\mathcal{O}_K/\mathfrak{p})$. Thus for each $\sigma \in I_\mathfrak{p}$ we have

$$\pi(\sigma(Q) - Q) = \sigma(\pi(Q)) - \pi(Q) = \pi(Q) - \pi(Q) = 0.$$

Since π is injective, it follows that $\sigma(Q) = Q$ for $\sigma \in I_\mathfrak{p}$, i.e., that Q is fixed under all $I_\mathfrak{p}$. This means that the subfield of L generated by the coordinates of Q is unramified at $\mathfrak{p}$. Repeating this argument with all choices of Q implies that L is unramified at $\mathfrak{p}$. □

Finally, we reach our ultimate destination.

Weak Mordell-Weil. We may assume all elements of $E[m]$ have coordinates in K, otherwise consider a finite Galois extension $L|K$ such that $E[m]$ have coordinates in L by Lemma 2.3. Then we have an injective homomorphism

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G_k, (\mathbb{Z}/m\mathbb{Z})^2).$$

By Theorem 2.11, the image consists of homomorphisms whose kernels cut out an abelian extension of K unramified outside m and primes of bad reduction for E. Since this is a finite set of primes, denoted as S, then $L := K^{K(S,m)}$ is finite by Theorem 2.9(Here we adopt the previous notation). Previous analysis impliles that the homomorphisms all factor through a finite group $\mathrm{Hom}(\mathrm{Gal}(L|K), (\mathbb{Z}/m\mathbb{Z})^2)$. Therefore the image of $E(K)/mE(K)$ is finite, which indicates $E(K)/mE(K)$ is finite. The proof is complete. □

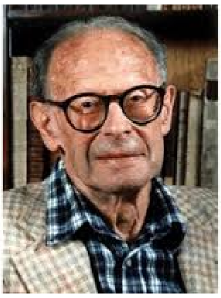

Figure 2: André Weil 1906-1998

References

[1] Gary Sivek, *The Analytic Class Number Formula*. gsivek@mit.edu, May 19,2005.

[2] Erich Hecke, *Lectures on the Theory of Algebraic Numbers*. Springer-Verlag, 1980. Print.

[3] Dinakar Ramakrishnan and Robert J. Valenza, *Fuourier Analysis on Number Fields*. Springer, 1991. Print.

[4] Serge Lang, *Algebraic Number Theory*. Springer-Verlag, 1986. Print.

[5] Li Siyan, *Elliptic curves and their torsion*, https://lsa.umich.edu/content/dam/math-assets/math-document/reu-documents/Li_Siyan%202014%20REU.pdf

[6] C.S. Rajan, *Weak Mordell-Weil Theorem*, http://www.math.tifr.res.in/~rajan/homepage/weakmorweil.pdf

[7] William Stein, *Introduction to algebraic number theory.* May 5, 2005.

[8] Silverman, Joseph H. *The Arithmetic of Elliptic Curves.* Springer, 2009. Print.

[9] Zheng Weizhe, *Lectures on Homological Algebra*, https://server.mcm.ac.cn/ zheng/homalg.pdf