

# Foundational Material for the Study of Elliptic Curves

Benjamin Church

March 29, 2023

## Contents

<b>1</b>	<b>Groups</b>	<b>2</b>
<b>2</b>	<b>Fields</b>	<b>3</b>
<b>3</b>	<b>Complex Analysis</b>	<b>3</b>
3.1	Holomorphic Functions . . . . .	3
3.2	Meromorphic Functions . . . . .	6

# 1 Groups

**Definition:** A group  $G$  is a set with a binary operation  $\circ$  which satisfies,

1. associativity,  $x \circ (y \circ z) = (x \circ y) \circ z$
2. there exists an identity  $e \in G$  such that  $e \circ g = g \circ e = g$  for any  $g \in G$
3. for each  $g \in G$  there exists an inverse  $g^{-1} \in G$  such that  $g \circ g^{-1} = g^{-1} \circ g = e$

**Example 1.1.** The following are groups,

1. the integers  $\mathbb{Z}$  with addition  $+$
2. the nonzero rational numbers  $\mathbb{Q}^\times$  with multiplication  $\cdot$
3. invertable matrices with matrix multiplication
4. the permutations of a set with composition of functions

**Definition:** We say that  $(G, \circ)$  is *abelian* if  $\circ$  is commutative,  $x \circ y = y \circ x$ . In this case we usually write  $x + y$  for the binary operation, 0 for  $e$  and  $-x$  for  $x^{-1}$  in analogy with the case of integers.

**Definition:** A group  $G$  is *finitely generated* if there exists a finite set  $S \subset G$  such that every element in  $g \in G$  can be expressed as a finite combination of elements of  $S$  (and the inverses of elements in  $S$ ) i.e.  $g = s_1 \circ \dots \circ s_n$  for  $s_1, \dots, s_n \in S \cup S^{-1}$  where  $S^{-1} = \{s^{-1} \mid s \in S\}$ .

**Example 1.2.** The following are groups,

1. the integers  $\mathbb{Z}$  are generated by one element, namely 1 so finitely generated.
2. the nonzero rational numbers  $\mathbb{Q}^\times$  with multiplication  $\cdot$  are not finitely generated since there are infinitely many prime numbers
3. invertable matrices with matrix multiplication are not finitely generated because they contain diagonal matrices with  $\mathbb{Q}^\times$  entries and these special matrices cannot be finitely generated by the above reason
4. the permutations of a finite set are finite in number and thus are obviously finitely generated.

**Remark 1.1.** Notice that the notion of being finitely generated is vacuous for finite groups.

**Definition:** A group that will be very important for us is the modular group  $SL_2(\mathbb{Z})$  is defined the group of matrices with integer coefficients and determinant one,

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$$

**Proposition 1.3.** The modular group is finitely generated with two generators,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

*Proof.* Exercise for you. □

**Remark 1.2.** If we have a group  $G$  and a subgroup  $H \subset G$  we would like a way to construct a smaller group by “sending  $H$  to zero.” We accomplish this by quotienting. However, we can only do this under the technical condition that the subgroup be normal.

**Definition:** Let  $H \subset G$  be a normal subgroup (meaning that  $gHg^{-1} \subset G$  for any  $g \in G$ ) then we define,

$$G/H = \{gH \mid g \in G\}$$

We call these sets  $gH$  cosets of  $H$ . Then they form a group via  $g_1H \cdot g_2H = g_1g_2H$ , one can show that this operation is well-defined exactly when  $H$  is normal in  $G$ . We define the index of  $H$  in  $G$  to be the size of this group,  $[G : H] = |G/H|$ .

**Example 1.4.** Modular arithmetic modulo  $n$ , taking the numbers  $0, 1, \dots, n-1$  and adding via “clock arithmetic” where  $n$  maps back around to  $0$  is accomplished via taking the subgroup of multiples of  $n$  in the integers  $n\mathbb{Z} \subset \mathbb{Z}$  and quotienting to get  $\mathbb{Z}/n\mathbb{Z}$ . This group has  $n$  elements so we say  $[\mathbb{Z} : n\mathbb{Z}] = n$ .

## 2 Fields

**Remark 2.1.** A field is an object that has the same algebraic structure as the rational numbers  $\mathbb{Q}$  or the real numbers  $\mathbb{R}$  or the complex numbers  $\mathbb{C}$ . It is a structure where we can add, subtract, multiply, and divide. In fields we can consider polynomials and if they have solutions. We will now give a formal definition.

**Definition:** A *field*  $(F, +, \cdot)$  is a set  $F$  with two binary operations  $+, \cdot$  and distinguished elements  $0, 1 \in F$  such that,

1.  $(F, +)$  is an abelian group with identity  $0$
2.  $(F^\times, \cdot)$  is an abelian group with identity  $1$  where  $F^\times = F \setminus \{0\}$  (in particular, every element but  $0$  has a multiplicative inverse)
3.  $\forall x, y, z \in F : x \cdot (y + z) = x \cdot y + x \cdot z$ .

## 3 Complex Analysis

### 3.1 Holomorphic Functions

**Definition:** A subset  $\Omega \subset \mathbb{C}$  is a domain if  $\Omega$  is open and connected.

**Definition:** A map  $f : \Omega \rightarrow \mathbb{C}$  is *holomorphic* at  $z \in \Omega$  if the limit,

$$f'(z) = \lim_{h \rightarrow 0} \frac{f(z+h) - f(z)}{h}$$

exists. The map  $f$  is holomorphic on  $\Omega$  if it is holomorphic at each  $z \in \Omega$ .

**Definition:** We say a map  $f : \mathbb{C} \rightarrow \mathbb{C}$  is *entire* if it is holomorphic on all of  $\mathbb{C}$ .

**Proposition 3.1.** Let  $f : \Omega \rightarrow \mathbb{C}$  be holomorphic at  $z \in \Omega$ . Then we may write  $f$  as a function of two real variables as,  $f(x, y) = f(x + iy)$ . This done,

$$f'(z) = \frac{\partial f}{\partial x} = \frac{1}{i} \frac{\partial f}{\partial y}$$

and thus,

$$\frac{\partial f}{\partial x} + i \frac{\partial f}{\partial y} = 0$$

**Definition:**

$$\frac{\partial f}{\partial z} = \frac{1}{2} \left[ \frac{\partial f}{\partial x} - i \frac{\partial f}{\partial y} \right] \quad \text{and} \quad \frac{\partial f}{\partial \bar{z}} = \frac{1}{2} \left[ \frac{\partial f}{\partial x} + i \frac{\partial f}{\partial y} \right]$$

Therefore, if  $f$  is holomorphic then

$$\frac{\partial f}{\partial z} = f'(z) \quad \text{and} \quad \frac{\partial f}{\partial \bar{z}} = 0$$

**Remark 3.1.** If we write  $f : \Omega \rightarrow \mathbb{C}$  in real form i.e. as a function  $F : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  with  $F(x, y) = (A(x, y), B(x, y))$  and  $f(x + iy) = A(x, y) + iB(x, y)$  then,

$$\frac{\partial f}{\partial \bar{z}} = \frac{1}{2} \left[ \frac{\partial f}{\partial x} + i \frac{\partial f}{\partial y} \right] = \frac{1}{2} \left[ \frac{\partial A}{\partial x} + i \frac{\partial B}{\partial x} + i \frac{\partial A}{\partial y} - \frac{\partial B}{\partial y} \right]$$

Therefore,

$$\frac{\partial f}{\partial \bar{z}} = 0 \iff \frac{\partial A}{\partial x} = \frac{\partial B}{\partial y} \quad \text{and} \quad \frac{\partial B}{\partial x} = -\frac{\partial A}{\partial y}$$

These are known as the Cauchy-Riemann equations. We will see that satisfying these equations along with some weak regularity is necessary and sufficient for a function to be holomorphic.

**Theorem 3.2.** Let  $\Omega$  be a domain and  $f : \Omega \rightarrow \mathbb{C}$ . Then the following are equivalent,

1.  $f : \Omega \rightarrow \mathbb{C}$  is holomorphic.
2.  $f$  is differentiable with continuous derivative and,

$$\frac{\partial f}{\partial \bar{z}} = 0$$

3. around the boundary of any disc  $D \subset \Omega$  we have,

$$\oint_{\partial D} f(z) \, dz = 0$$

**Theorem 3.3.** Let  $\Omega$  be a domain and  $f : \Omega \rightarrow \mathbb{C}$ . Then the following are equivalent,

1.  $f : \Omega \rightarrow \mathbb{C}$  is holomorphic.
2.  $f \in \mathcal{C}^1(\Omega)$  and

$$\frac{\partial f}{\partial \bar{z}} = 0$$

3.  $f \in \mathcal{C}^1(\Omega)$  and for  $D \subseteq \Omega$  with piecewise  $\mathcal{C}^1(\Omega)$  boundary we have

$$\oint_{\partial D} f(z) \, dz = 0$$

4.  $\forall B_r(w) \subset \subset \Omega$  we have,

$$f(z) = \frac{1}{2\pi i} \oint_{\partial B_r(w)} \frac{f(\zeta)}{\zeta - z} \, d\zeta$$

for all  $z \in B_r(w)$ .

5.  $f$  is complex analytic:  $\forall w \in \Omega : \exists r > 0$  such that whenever  $|z - w| < r$  we have,

$$f(z) = \sum_{n=0}^{\infty} a_n (z - w)^n$$

**Theorem 3.4** (Cauchy). Let  $f : \Omega \rightarrow \mathbb{C}$  be holomorphic, for any disc  $D \subset \Omega$  and  $w \in D^\circ$  we have,

$$f^{(n)}(w) = \frac{n!}{2\pi i} \oint_{\partial D} \frac{f(z)}{(z-w)^{n+1}} dz$$

In particular, the coefficients of the series expansion about  $w$  are,

$$a_n = \frac{1}{2\pi i} \oint_{\partial D} \frac{f(z)}{(z-w)^{n+1}} dz$$

**Lemma 3.5.** For any  $z_0 \in \Omega$ , either  $f \equiv 0$  in a neighborhood of  $z_0$  or we can express  $f = (z-z_0)^n u(z)$  for  $u(z)$  holomorphic and  $u(z) \neq 0$ .

*Proof.* In a neighborhood of  $z_0$ , we can write,

$$f(z) = \sum_{n=0}^{\infty} c_n (z-z_0)^n$$

Either  $c_n = 0$  for each  $n$  so  $f = 0$  or  $c_N \neq 0$  for some  $n$  and  $c_n = 0$  for  $n < N$ . Therefore,

$$f(z) = \sum_{n \geq N} c_n (z-z_0)^n = (z-z_0)^N \left( \sum_{m=0}^{\infty} c_{N+m} (z-z_0)^m \right) = (z-z_0)^N u(z)$$

Furthermore,  $u(z_0) = c_N \neq 0$  so there exists a neighborhood of  $z_0$  on which  $u(z) \neq 0$ .  $\square$

**Proposition 3.6.** Let  $f : \Omega \rightarrow \mathbb{C}$  be holomorphic (and not identically zero) then the set of zeros,  $f^{-1}(0)$  is discrete.

*Proof.* Let  $f$  vanish at  $z_0$ . If  $f$  were identically zero on some open neighborhood of  $z_0$  then  $f$  would be identically zero on  $\Omega$ . Thus, by the lemma, we can write  $f = (z-z_0)^n u(z)$  on some open neighborhood  $U$  of  $z_0$  where  $u(z)$  is nonvanishing on  $U$ . Furthermore,  $(z-z_0)^n$  vanishes exactly at  $z_0$  so we have  $f^{-1}(0) \cap U = \{z_0\}$  implying that  $f^{-1}(0)$  is discrete.  $\square$

**Corollary 3.7.** Let  $f$  be a nonconstant holomorphic function. Then on any bounded set  $f$  has finitely many zeros.

**Theorem 3.8** (Liouville). Every bounded entire<sup>1</sup> function is constant.

*Proof.* Let  $f : \mathbb{C} \rightarrow \mathbb{C}$  be entire and bounded everywhere by  $M$ . Take  $w \in \mathbb{C}$  and let  $C$  be a circle around  $z$  with radius  $R$ . Then applying the Cauchy integral formula,

$$f'(w) = \frac{1}{2\pi i} \oint_C \frac{f(z)}{(z-w)^2} dz = \frac{1}{2\pi} \int_0^{2\pi} \frac{f(w + Re^{i\theta})}{R^2 e^{2i\theta}} R d\theta$$

Therefore,

$$|f'(w)| = \frac{1}{2\pi} \left| \oint_C \frac{f(z)}{(z-w)^2} dz \right| \leq \frac{1}{2\pi} \int_0^{2\pi} \frac{|f(w + Re^{i\theta})|}{R^2} R d\theta \leq \frac{1}{2\pi} \int_0^{2\pi} \frac{M}{R} d\theta = \frac{M}{R}$$

which goes to zero in the limit  $R \rightarrow \infty$ . Since  $R$  is arbitrarily large,  $f'(w) = 0$  so  $f$  is constant since it has zero derivative everywhere.  $\square$

---

<sup>1</sup>holomorphic on the entire complex plane

### 3.2 Meromorphic Functions

**Definition:** A function  $f : \Omega \rightarrow \mathbb{C}$  is meromorphic if, near any  $z_0 \in \Omega$ , it can be written as,

$$f(z) = \sum_{n \geq -N} c_n (z - z_0)^n$$

We call  $N$  the order of the pole (assuming that  $c_n \neq 0$ ) and  $c_{-1}$  the residue at  $z_0$ . This expansion shows that  $f$  must have isolated poles and zeros.

**Theorem 3.9.** Meromorphic functions  $h : \Omega \rightarrow \mathbb{C}$  are exactly ratios of holomorphic functions,

$$h(z) = \frac{f(z)}{g(z)}$$

Since  $g$  is holomorphic it has isolated zeros and thus  $h$  has isolated poles.

**Theorem 3.10 (Residue).** Let  $f : \Omega \rightarrow \mathbb{C}$  be meromorphic and  $D \subset \overline{D} \subset \Omega$  be a domain in  $\Omega$  with piecewise smooth boundary  $\partial D$  such that no poles of  $g$  lie on  $\partial D$ . Then,

$$\oint_{\partial D} f(z) dz = 2\pi i \sum_{p \in D} \text{Res}_p f$$

*Proof.* We can deform the path  $\partial D$  to a sum of small circles of radius  $r$  surrounding each pole. Since  $f$  is holomorphic on the region  $D$  minus these circles the two integrals along these paths (whose difference is the integral over the boundary) are equal. Thus,

$$\begin{aligned} \oint_{\partial D} f(z) dz - 2\pi i \sum_{p \in D} \text{Res}_p f &= \sum_{p \in D} \left[ \oint_{\partial B_r(p)} f(p+z) dz - 2\pi i \text{Res}_p f \right] \\ &= \sum_{p \in D} \left[ \int_0^{2\pi} i \left( f(p + re^{i\theta}) re^{i\theta} - \text{Res}_p f \right) d\theta \right] \end{aligned}$$

However,

$$\text{Res}_p f = \lim_{z \rightarrow p} (z - p) f(z) = \lim_{h \rightarrow 0} f(p + h) h$$

and thus, for each  $\epsilon > 0$  we can choose some  $\delta$  such that  $r < \delta$  implies that,

$$|f(p + re^{i\theta}) re^{i\theta} - \text{Res}_p f| < \epsilon$$

Therefore,

$$\begin{aligned} \left| \oint_{\partial D} f(z) dz - 2\pi i \sum_{p \in D} \text{Res}_p f \right| &\leq \sum_{p \in D} \left[ \int_0^{2\pi} |f(p + re^{i\theta}) re^{i\theta} - \text{Res}_p f| d\theta \right] \\ &\leq \sum_{p \in D} \int_0^{2\pi} \epsilon d\theta = 2\pi N \epsilon \end{aligned}$$

where  $N$  is the number of poles. Since  $\epsilon$  is arbitrary,

$$\oint_{\partial D} f(z) dz = 2\pi i \sum_{p \in D} \text{Res}_p f$$

□

**Theorem 3.11.** Let  $f : \Omega \rightarrow \mathbb{C}$  be meromorphic and  $D \subset \overline{D} \subset \Omega$  be a domain in  $\Omega$  with piecewise smooth boundary  $\partial D$  such that no poles of  $g$  lie on  $\partial D$ . Then,

$$\frac{1}{2\pi i} \oint_{\partial D} \frac{f'(z)}{f(z)} dz = (\# \text{ of zeros}) - (\# \text{ of poles})$$

*Proof.* At each point  $p \in D$  we can expand,

$$f(z) = (z - p)^N u(z)$$

where  $u$  is holomorphic and nonvanishing. Therefore,

$$\frac{f'(z)}{f(z)} = \frac{d}{dz} \log f(z) = \frac{d}{dz} [(z - p)^N u(z)] = \frac{N}{z - p} + \frac{u'(z)}{u(z)}$$

Thus when  $f$  has either a zero ( $N > 0$ ) or a pole ( $N < 0$ ) the logarithmic derivative has residue,

$$\text{Res}_p \left( \frac{f'}{f} \right) = N$$

Therefore the result holds by the residue theorem.  $\square$

**Corollary 3.12.** Let  $f : \Omega \rightarrow \mathbb{C}$  be holomorphic take  $w \in \mathbb{C}$ , then the number of solutions in  $D$  to the equation  $f(z) - w = 0$  is equal to,

$$\#\{z \in D \mid f(z) = w\} = \oint_{\partial D} \frac{f'(z)}{f(z) - w} dz$$

*Proof.* Since  $f - w$  is holomorphic on  $\Omega$  it has no poles. Therefore, the only residues are from roots of  $f - w$  i.e. solutions to  $f(z) - w = 0$ . As above, the integral of the logarithmic derivative counts the number of such poles.  $\square$