Number theory and arithmetic geometry

Soham Chowdhury

July 28, 2017

Contents

Part I

Basic notions

Chapter 1

Category theory

Chapter 2

Sheaves

Chapter 3

Affine schemes

3.1 Motivation

3.2 The spectrum of a ring

Define

$$\mathsf{Spec}\, R = \{I \subseteq R : I \text{ is a prime ideal}\}$$

3.3 Some examples

Chapter 4

Algebraic integers

> Pellentesque condimentum,
> magna ut suscipit hendrerit,
> ipsum augue ornare nulla, non
> luctus diam neque sit amet urna.
>
> The Dude

Fix a domain A integrally closed in $K := K(A)$. Let $L|K$ be a finite extension, and B the integral closure of A in L. This is the $AKLB$ *diagram*:

$$\begin{tikzcd} K \arrow[r, hook] & L \\ A \arrow[u] \arrow[r] & B \arrow[u] \end{tikzcd}$$

4.1 Properties of integrality

Integrality is stable under the ring operations: one would like the following to hold, and they do:
This is a corollary of the following:

Theorem 4.1.1 (Module-theoretic characterization of integrality)**.** *A finite number of b_i are integral over $A \iff$ the ring $A[b_1, \dots, b_n]$ is finitely generated as an A-module.*

Proof. TODO. ∎

Corollary 4.1.2. *If a and b are integral over A, so are $a + b$ and ab.*

Theorem 4.1.3 (Integrality is transitive)**.** *Consider ring extensions $A \subseteq B \subseteq C$. $A \subseteq B$ integral and $B \subseteq C$ integral $\iff$ $A \subseteq C$ integral.*

Proof. $A \subseteq C$ integral implies $A \subseteq B$ integral. (Why?) ∎

Theorem 4.1.4. *Any element $l \in L$ is equal to b/a for $b \in B$ and $a \in A$.*

Proof. Consider an element $l \in L$. The minimal polynomial m_l of l over K gives rise to a polynomial over A

$$a_n l^n + a_{n-1} l^{n-1} + \cdots + a_0 = 0$$

by clearing denominators. Now observe that $\ell := a_n l$ is integral over A: multiplying by a_n^{n-1} gives an equation of the form

$$\ell^n + a'_{n-1} \ell^{n-1} + \cdots + a'_0 = 0.$$

This shows that taking $b/a = \ell/a_n$ works. ∎

Remark 4.1.5. Notice that $K(B) = L$. Indeed, $B \subset L$ so $K(B) \subset L$, and the result above shows that $L \subset K(B)$ (set-theoretically, $L \subset B \times A \subset B \times B$).

Theorem 4.1.6. *$l \in L$ is integral over A iff its minimal polynomial μ_l over K has coefficients in A.*

Proof. If $\mu := \mu_l \in A[x]$ then we have integrality of l over A by definition. Consider now the case of an integral l with minimal polynomial $\mu \in K[x]$. From integrality over A we know that l is a root of some $g \in A[x]$. Then $\mu|g$ in $K[x]$, so all zeros of μ are zeros of g and hence integral over A.

By Vietà, the coefficients a_i are given by elementary symmetric polynomials in the roots and are hence, by Corollary 4.1.2, integral over A themselves. The a_i are elements of K, so, in this case, integrality over A means that $a_i \in K$, and hence $\mu \in A[x]$. ■

4.2 The trace and the norm

Given $x \in L$, multiplication by x determines an endomorphism

$$T_x : \alpha \mapsto x\alpha$$

of the K-vector space L. We define the trace and norm maps

$$\begin{aligned} \mathrm{Tr}_{L|K}(z) &= \mathrm{tr}\, T_z \\ \mathrm{Nm}_{L|K}(z) &= \det T_z \end{aligned}$$

Let $n = [L : K]$. The characteristic polynomial

$$\begin{aligned} \chi_z(t) &= \det(tI - T_z) \\ &= t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[i] \end{aligned}$$

contains coefficients $a_1 = \mathrm{Tr}_{L|K}(z)$ and $a_n = \mathrm{Nm}_{L|K}(z)$.

Remark 4.2.7. If this isn't immediately clear, think Vietà. (This will be one of the recurring themes throughout this chapter.)

4.3 Galois-theoretic interpretations

Fix an algebraic closure $\bar{K} = K^{alg}$ of K.

Proposition 4.3.8. *If $L|K$ is separable, letting $\sigma : L \to \bar{K}$ vary over the K-embeddings of L into $\bar{K}$, we have*

1. $\chi_z(t) = \prod_\sigma (t - \sigma z)$
2. $\mathrm{Tr}_{L|K}(z) = \sum_\sigma \sigma z$
3. $\mathrm{Nm}_{L|K}(z) = \prod_\sigma \sigma z$

Proof. Let $d = [L : K(x)]$. The characteristic polynomial is a power

$$\chi_z = \mu_z^d$$

where $d = [L : K(z)]$. Part 1 easily implies the others, by Vietà's formulas. ■

Theorem 4.3.9. *For a tower of finite extensions $K \subseteq L \subseteq M$, we have*

$$\begin{aligned} \mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L} &= \mathrm{Tr}_{M|K} \\ \mathrm{Nm}_{L|K} \circ \mathrm{Nm}_{M|L} &= \mathrm{Nm}_{M|K} \end{aligned}$$

4.4 Integral bases

Definition 4.4.10. *The* **discriminant** *of a basis α_i of a separable extension $L|K$ is defined by*

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j))^2$$

where the σ_i are the K-embeddings $L \hookrightarrow \bar{K}$.

Proposition 4.4.11. *For $L|K$ a separable extension with basis α_i, the function*

$$(x, y) = \mathrm{Tr}_{L|K}(xy)$$

yields a nondegenerate bilinear form on the K-vector space L.

Corollary 4.4.12. *For $L|K$ and α_i as above,*

$$d(\alpha_1, \ldots, \alpha_n) \neq 0.$$

Proof. The form has matrix

$$M = \mathrm{Tr}_{L|K}((\alpha_i \alpha_j))$$

with respect to the given basis. The nondegeneracy of the form, which we have from Proposition 4.4.11, is equivalent to the statement that $\det M \neq 0$, whence the claim follows. ■

Lemma 4.4.13. *Let (α_i) be a basis of $L|K$ contained in B, with $d = d(\alpha_1, \ldots, \alpha_n)$. Then*

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Proposition 4.4.14. *If $L|K$ is separable and A is a PID, every finitely generated B-submodule $M \neq 0$ of L s a free A-module of rank $[L : K]$.*

Corollary 4.4.15. *B admits an integral basis over A.*

Proposition 4.4.16. *Let $M|K$ and $N|K$ be two Galois extensions with $M \cap N = K$, with $m = [M : K]$ and $n = [N : K]$. Fix integral bases $(\alpha_i)_{1 \leqslant i \leqslant m}$ of $M|K$ and $(\beta_j)_{1 \leqslant j \leqslant n}$ of $N|K$ respectively, with discriminants μ and ν respectively. If μ and ν are relatively prime, with $x\mu + y\nu = 1$ for some $x, y \in A$, then $(\alpha_i \beta_j)$ is an integral basis of MN, with discriminant $m^\nu n^\mu$.*

Proposition 4.4.17. *If $\mathfrak{i} \subseteq \mathfrak{j}$ are two nonzero finite $\mathcal{O}_K$-submodules of K, then $(\mathfrak{j} : \mathfrak{i})$ is finite. Moreover,*

$$d(\mathfrak{i}) = (\mathfrak{j} : \mathfrak{i})^2 d(\mathfrak{j})$$

holds.

Appendix A

Commutative algebra

A.1 Tensor products of modules

A.2 Operations on modules

A.3 Localization

Appendix B

Complex analysis

B.1 Holomorphy and complex differentiability

There are, broadly speaking, two criteria that we would like nice complex-valued functions to satisfy. The first is a notion of differentiability similar to the one from calculus, where every function can be linearly approximated by a *derivative*, while the second asks that every function be locally representable by a *power series* expansion.

This section will develop these notions, demonstrate relations between the two, and discuss some simple consequences of these conditions.

Initial definitions

Let $\Omega \subseteq \mathbf{C}$ be an open set.

Definition B.1.1. *A function* $f : \Omega \to \mathbf{C}$ *is* complex differentiable at z_0 *if the limit*

$$f'(z_0) = \lim_{h \to 0} \frac{f(z_0 + h) - f(z_0)}{h}$$

exists. f *is said to be* complex differentiable on Ω *if it is complex differentiable at all* $z_0 \in \Omega$*.*

Definition B.1.2 (Narasimhan)**.** $f : \Omega \to \mathbf{C}$ *is* holomorphic on Ω *if, for all* $z_0 \in \Omega$*, there exists a neighborhood* $U \subseteq \Omega$ *of* z_0 *and a sequence* $\{c_n\}_{n \geqslant 0}$ *of complex numbers such that, for all* $z \in U$*, the series*

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

converges to $f(z)$*.*

These two definitions are in fact equivalent: holomorphy on Ω is the same as $\mathbf{C}$-differentiability on Ω. This is the content of the Cauchy-Goursat theorem, which we will prove later (TODO ref).

Properties

Holomorphy and complex differentiability imply relations between the "x-behavior" and "y-behavior" of a function, so that there are certain rigidity properties we can be assured of. We now show a few properties which are all roughly similar in nature, culminating in Definition B.1.6.

Proposition B.1.3. *Let* $f : \Omega \to \mathbf{C}$ *be* $\mathbf{C}$*-differentiable at* $a \in \Omega$*. Then* $\partial_x f(a)$ *and* $\partial_y f(a)$ *exist, and*

$$\frac{\partial f}{\partial x}(a) = -i \frac{\partial f}{\partial y}(a) = f'(a)$$

holds.

Proof. In the Riemann tradition, write $a = \sigma + it$. We will calculate $f'(a)$ in two ways, by approaching 0 along the real axis, then along the imaginary axis.

Taking $0 \neq \xi \in \mathbf{R}$,

$$\begin{aligned} f'(a) &= \lim_{\xi \to 0} \frac{f(a+\xi) - f(a)}{\xi} \\ &= \lim_{\xi \to 0} \frac{f(\sigma + \xi, t) - f(\sigma, t)}{\xi} \\ &= \frac{\partial f}{\partial x}(a). \end{aligned}$$

Taking $0 \neq \eta \in \mathbf{R}$,

$$\begin{aligned} f'(a) &= \lim_{\xi \to 0} \frac{f(a+\eta) - f(a)}{i\eta} \\ &= \lim_{\xi \to 0} \frac{f(\sigma, t + \eta) - f(\sigma, t)}{i\eta} \\ &= \frac{1}{i} \frac{\partial f}{\partial y}(a). \end{aligned}$$

Equating these two expressions to $f'(a)$ is then enough. ∎

Note that x and y can be expressed in terms of z and $\bar{z}$:

$$\begin{aligned} x &= \frac{z + \bar{z}}{2} \\ y &= \frac{z - \bar{z}}{2i} \end{aligned}$$

This means one can (formally?) write, using the chain rule,

$$\frac{\partial f}{\partial z} = \frac{\partial f}{\partial x}\frac{\partial x}{\partial z} + \frac{\partial f}{\partial y}\frac{\partial y}{\partial z} = \frac{1}{2} \cdot \frac{\partial f}{\partial z} + \frac{1}{2i} \cdot \frac{\partial f}{\partial y} = \frac{1}{2}(f_z - i f_y)$$

Exercise B.1.A. *What is the analogous expression for $\partial_{\bar{z}}$?*

This motivates the following definition.

Definition B.1.4. *The* Wirtinger derivatives *are differential operators defined as follows:*

$$\begin{aligned} \partial_z &= \frac{\partial}{\partial z} = \frac{1}{2}(\partial_x - i\partial_y) \\ \partial_{\bar{z}} &= \frac{\partial}{\partial \bar{z}} = \frac{1}{2}(\partial_x + i\partial_y) \end{aligned}$$

Proposition B.1.5. *If $f : \Omega \to \mathbf{C}$ is $\mathbf{C}$-differentiable at $a \in \Omega$,*

$$\begin{aligned} \frac{\partial f}{\partial z}(a) &= f'(a) \\ \frac{\partial f}{\partial \bar{z}}(a) &= 0 \end{aligned}$$

Exercise B.1.B. *Prove this. (This is essentially a restatement of Proposition B.1.3 using the new notation.)*

Definition B.1.6. *Let $f : \Omega \to \mathbf{C}$ be written as $f = u + iv$, where $u, v : \Omega \to \mathbf{R}$. Then the equations*

$$\begin{aligned} \frac{\partial f}{\partial x} &= i\frac{\partial f}{\partial y} \\ \frac{\partial f}{\partial z} &= \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial \bar{z}} &= 0 \end{aligned}$$

are each equivalent to the following pair of equations:

$$u_x = v_y \tag{B.1}$$
$$-u_y = v_x \tag{B.2}$$

These differential equations are called the Cauchy-Riemann equations*.*

Define an $\mathbf{R}$-isomorphism of fields

$$\begin{aligned} \mu : \mathbf{C} &\to \mathbf{R}^2 \\ x + iy &\mapsto (x, y) \end{aligned}$$

Let $f : \Omega \to \mathbf{C}$ have first partial derivatives at w. We have the *Jacobian map*, represented in the standard basis by

$$J_w(u, v) = \begin{bmatrix} u_x(w) & u_y(w) \\ v_x(w) & v_y(w) \end{bmatrix}$$

This is a local isomorphism of $\mathbf{R}^2$ onto the tangent space $T_w\mathbf{R}^2 \simeq \mathbf{R}^2$. We "lift" this to $\mathbf{C}$:

Definition B.1.7. *The* tangent map *of* $f = u + iv$ *at* w *is*

$$d_w f := \mu^{-1} \triangleleft J_w(u, v) \triangleleft \mu$$

Proposition B.1.8. *We have* $\partial_{\bar{z}} f(w) = 0$ *iff* $d_w f$ *is* $\mathbf{C}$*-linear, that is, if*

$$d_w f(\lambda \cdot z) = \lambda \cdot d_w f(z)$$

in which case

$$d_w f(z) = z \cdot \partial_z f(w) = z \cdot f'(w)$$

Notice that this says exactly that f is locally linear.

Proof. TODO. Pretty weird in Narasimhan. ∎

$\mathbf{C}$-differentiable functions satisfy the expected properties:

1. Given differentiable $f, g : \Omega \to \mathbf{C}$ and $\lambda \in \mathbf{C}$,

$$\begin{aligned} f + g &: z \mapsto f(z) + g(z) \\ f \cdot g &: z \mapsto f(z) \cdot g(z) \\ \lambda \cdot f &: z \mapsto \lambda \cdot f(z) \end{aligned}$$

   are all $\mathbf{C}$-differentiable.

2. Consider open sets U, V in $\mathbf{C}$. If $f : U \to \mathbf{C}$ and $g : V \to \mathbf{C}$ are complex differentiable, then $g \triangleleft f : U \to \mathbf{C}$ is complex differentiable if it is defined — that is, if $f(U) \subseteq V$. Further, for $z_0 \in U$, we have a *chain rule*:

$$(g \triangleleft f)' = (g' \triangleleft f) \cdot f'$$

Recall that a function is C^k on some domain if all partial derivatives of orders $\leqslant k$ exist and are continuous.

Proposition B.1.9. *Let* $f : \Omega \to \mathbf{C}$ *be* C^1 *and satisfy the Cauchy-Riemann equations on* Ω*. Then* f *is* $\mathbf{C}$*-differentiable on* Ω*.*

In fact, the partial derivatives only need to exist: the Looman–Menchoff theorem (TODO ref) says that they need not be assumed to be continuous themselves.

Proof. Let $\zeta = \xi + i\eta$. Write $f = u + iv$, and let $w = \alpha + i\beta \in \Omega$. Using Taylor's theorem for C^1 functions,

$$\begin{aligned} u(w+\zeta) - u(w) &= \tilde{u}(\alpha + \zeta, \beta + \eta) - \tilde{u}(\alpha, \beta) \\ &= \frac{\partial \tilde{u}}{\partial x}(\alpha, \beta) \cdot \xi + \frac{\partial \tilde{u}}{\partial y}(\alpha, \beta) \cdot \eta + \varepsilon_1(\xi, \eta) \\ &= \frac{\partial u}{\partial x}(w) \cdot \xi + \frac{\partial u}{\partial y}(w) \cdot \eta + \varepsilon_1(\xi, \eta) \end{aligned}$$

Similarly, we have

$$v(w+\zeta) - v(w) = \frac{\partial u}{\partial x}(w) \cdot \xi + \frac{\partial u}{\partial y}(w) \cdot \eta + \varepsilon_2(\xi, \eta)$$

Crucially, as $\xi, \eta \to 0$, we have the bounds

$$\begin{aligned} \frac{\varepsilon_1(\xi,\eta)}{|\xi| + |\eta|} &\to 0 \\ \frac{\varepsilon_2(\xi,\eta)}{|\xi| + |\eta|} &\to 0 \\ \frac{\varepsilon(\xi,\eta)}{|\zeta|} &\to 0 (how?) \end{aligned}$$

where $\varepsilon = \varepsilon_1 + i\varepsilon_2$.
We combine the previous two equations to get

$$f(w+\zeta) - f(w) = f_x(w) \cdot \xi + f_y(w) \cdot \eta + \epsilon(\zeta)$$

and, using the Cauchy-Riemann equations to write f_y as if_x, we see that the limit

$$\begin{aligned} \lim_{\zeta \to 0} \frac{f(w+\zeta) - f(w)}{\zeta} &= \frac{f_x(w) \cdot (\xi + i\eta)}{\zeta} + \lim_{\zeta \to 0} \frac{\epsilon(\zeta)}{\zeta} \\ &= \frac{\partial f}{\partial x}(w) \end{aligned}$$

exists (and is differentiable?). ∎

Erratum B.1. *In his proof of Proposition B.1.9, where Narasimhan writes $\zeta = \zeta + i\eta$, he means $\zeta = \xi + i\eta$.*

B.2 Power series

Lemma B.2.10 (Abel)**.** *Given a sequence $\{c_n\}_{n \geqslant 0}$ in $\mathbf{C}$, there exists $0 \leqslant R \in \mathbf{R}_\infty = \mathbf{R} \cup \{\infty\}$ such that the series*

$$\sum_{n=0}^{\infty} c_n z^n$$

*converges for $|z| < R$ and diverges for $|z| > R$. Further, the series converges **uniformly** on any compact subset of $D_R(0)$.*

This means that, given any power series, there exists a disc inside which it converges and outside which it diverges. Abel's lemma does not say what will happen on the boundary circle $|z| = R$ (funny things do sometimes).

Proof. Choose

$$R = \sup \{r \geqslant 0 : \exists M. \forall n \geqslant 0. |c_n| r^n \leqslant M\}$$

or, in words, R is the "biggest" disc inside which $|c_n||z|^n$ is bounded. By construction,

$$|z| > R \implies |c_n||z|^n \text{ is not bounded}$$

so (why? TODO) $\sum c_n z^n$ cannot converge.

Let $K \subseteq D_R$ be compact. Choose $\rho < R$ such that $K \subseteq D_\rho$, and r such that $\rho < r < R$. There exists (?) $M > 0$ such that $|c_n| r^n \leqslant M$. For $z \in K$,

$$|c_n z^n| \leqslant |c_n|\rho^n \leqslant M\left(\frac{\rho}{r}\right)^n$$

Since $\rho < r$, we have $M\sum\left(\frac{\rho}{r}\right)^n < \infty$, so that $\sum c_n z^n$ converges uniformly on K.

■

Definition B.2.11. *The real number* R *is called the* radius of convergence *of* $\sum_{n=0}^{\infty} c_n z^n$.

Corollary B.2.12. *Holomorphy on an open set* $\Omega \subseteq \mathbf{C}$ *implies continuity on* Ω.

Lemma B.2.13. *The radius of convergence of*

$$\sum_{n=1}^{\infty} n c_n z^{n-1}$$

is equal to that of

$$\sum_{n=0}^{\infty} c_n z^n.$$

Proof. ■

Derivatives of power series

Lemma B.2.14. *Let* $a, b \in \mathbf{C}$. *We have*

$$|(a+b)^n - a^n| \leqslant n|b|\left(|a|+|b|\right)^{n-1}$$

for $n \geqslant 1$.

Proof. From high-school algebra, we have the factorization

$$\begin{aligned}(a+b)^n - a^n &= (a+b-a)\sum_{k=0}^{n-1}(a+b)^{n-1-k} - a^k \\ &= b\sum_{k=0}^{n-1}(a+b)^{n-1}\left(\frac{a}{a+b}\right)^k\end{aligned}$$

We take absolute values of both sides and apply the triangle inequality:

$$\begin{aligned}|(a+b)^n - a^n| &= |b|\left|\sum_{k=0}^{n-1}(a+b)^{n-1}\left(\frac{a}{a+b}\right)^k\right| \\ &\leqslant |b|\sum_{k=0}^{n-1}|a+b|^{n-1}\left|\frac{a}{a+b}\right|^k \\ &\leqslant |b|\sum_{k=0}^{n-1}|a+b|^{n-1} \\ &= n|b|(|a|+|b|)^{n-1}\end{aligned}$$

■

Proposition B.2.15. *Let* $R > 0$, *and consider a power series*

$$\sum_{n=0}^{\infty} c_n(z-z_0)^n \to f(z) \quad \textit{for } z \in D_R(z_0)$$

Then f *is* $\mathbf{C}$*-differentiable on* $D_R(z_0)$ *and*

$$f'(z) = \sum_{n=1}^{\infty} n c_n(z-z_0)^{n-1} \textit{ for } z \in D_R(z_0)$$

Proof. Let $z \in D_R(z_0)$. Set

$$R_\pm = \frac{1}{2}(R \pm |z - z_0|)$$

and choose a complex number ζ satisfying $0 < |\zeta| < R_-$. Then

$$\frac{f(z+\zeta) - f(z)}{\zeta} = \sum_{n=1}^{\infty} c_n \frac{(z+\zeta-z_0)^n - (z-z_0)^n}{\zeta}$$

Let $N > 0$. By Lemma B.2.14,

$$\begin{aligned}\left|\sum_{n>N} c_n \frac{(z+\zeta-z_0)^n - (z-z_0)^n}{\zeta}\right| &\leqslant \sum_{n>N} n|c_n|(|\zeta| + |z-z_0|)^{n-1} \\ &\leqslant \sum_{n>N} n|c_n|R_+^{n-1}\end{aligned}$$

Since $R_- \leqslant R \leqslant R_+$, $|z - z_0| < R_+$.

$$\begin{aligned}&\left|\frac{f(z+\zeta) - f(z)}{\zeta} - \sum_{n=1}^{\infty} nc_n(z-z_0)^{n-1}\right| \\ &= \left|\frac{f(z+\zeta) - f(z)}{\zeta} - \sum_{n=1}^{N} nc_n(z-z_0)^{n-1} - \sum_{n>N} nc_n(z-z_0)^{n-1}\right| \\ &= \left|\sum_{n=0}^{\infty} c_n \frac{(z+\zeta-z_0)^n - (z-z_0)^n}{\zeta} - \sum_{n=1}^{N} nc_n(z-z_0)^{n-1} - \sum_{n>N} nc_n(z-z_0)^{n-1}\right| \\ &\leqslant \sum_{n=1}^{N} |c_n| \left|\frac{(z+\zeta-z_0)^n - (z-z_0)^n}{\zeta} - n(z-z_0)^{n-1}\right| + 2\sum_{n>N} n|c_n|R_+^{n-1}\end{aligned}$$

■

B.3 Contour integration

Definition B.3.16. *Let $\gamma : [a, b] \to \Omega \subseteq \mathbf{C}$ be piecewise differentiable. The length $L(\gamma)$ of γ is*

$$L(\gamma) := \int_a^b |\gamma'(t)|\, dt$$

Proposition B.3.17. *Let $\Omega \subseteq \mathbf{C}$ be open and $f \in C^1(\Omega)$. Let $R \subset \Omega$ be a closed rectangle. Then*

$$\iint_R \frac{\partial f}{\partial \bar{z}}\, dx\, dy = -\frac{i}{2} \int_{\partial R} f\, dz$$

Proof. Let $R = [a, b] \times [c, d]$, with vertices $v_{1,\ldots,4}$ and sides $\gamma_{1,\ldots,4}$. ■

B.4 Zeroes and poles

Definition B.4.18 (Zeros)**.**

Definition B.4.19. *A function $f : \mathbf{C} \to \mathbf{C}$ is* elliptic *if, for all λ in some lattice Λ, $f(z + \lambda) = f(z)$ for all $z \in \mathbf{C}$.*

Theorem B.4.20 (Liouville)**.** *Any bounded entire function is constant.*

Definition B.4.21. *If f is holomorphic on all of $\mathbf{C}$, it is said to be* entire*.*

Appendix C

Fourier analysis

C.1 Fourier expansions

Let $g : \mathbf{C} \to \hat{\mathbf{C}}$ be a continuous function with period 1.
The nth *Fourier coefficient* $a_n(y)$ is

$$a_n(y) = \hat{g}(n) = \int_0^1 g(z)\exp(-2\pi i n z)dx$$

Then we have the *Fourier expansion*

$$g(z) = \sum_{n=-\infty}^{\infty} a_n(y)\exp(2\pi i n z)$$

C.2 Meromorphy

The *nome* is a common building block for interesting functions.

$$q = q(z) := \exp(2\pi i z)$$

Let g be meromorphic in the notation of the previous section. Then there exists a unique meromorphic $G : \mathbf{C}^\times \to \hat{\mathbf{C}}$ such that $g(z) = G(q)$ (TODO why?): in other words, a period-1 meromorphic function of z is in fact a function of $q(z)$.
Note that G has a removable singularity at 0, so, by Theorem ???, G extends to a meromorphic function on $\mathbf{C}$ iff

$$\lim_{q\to 0} G(q)|q|^m = 0$$

for some m. What does it mean for q to go to 0?

$$\begin{aligned} q \to 0 &\implies \exp(2\pi i(x+iy)) \to 0 \\ &\implies \exp(2\pi i x)e^{-2\pi y} \to 0 \\ &\implies y \to \infty \end{aligned}$$

so we have $g(z)|q|^m \to 0$ as $g(z)\exp(-2\pi m y) \to 0$, so we need

$$\text{as } \Im(z) \to \infty, \exists m \;\; |g(z)| < \exp(2\pi m y)$$

The meromorphy of $G(q)$ at 0 thus requires $\Im(z) \to \infty$, in which case we say g is *meromorphic at* $i\infty$. Then G, being meromorphic at 0, has a Laurent series expansion

$$g(z) = G(q) = \sum_{n=-m}^{\infty} c_n q^n = \sum_{n=-m}^{\infty} c_n e^{2\pi i n z}$$

Here m is the order of the pole of G at 0. However, we also have a Fourier expansion

$$g(z) = \sum_{n=-\infty}^{\infty} a_n(y) e^{2\pi i n z}$$

and, equating coefficients,

$$\begin{aligned} a_n(y) &= c_n && \text{for } n \geqslant -m \\ a_n(y) &= 0 && \text{for } n < -m \end{aligned}$$

Appendix D

Modular forms

D.1 The hyperbolic plane

Definition D.1.1. *The* upper half-plane *in* $\mathbf{C}$ *is*

$$\mathfrak{H} := \{h \in \mathbf{C} : \operatorname{Im}(h) > 0\}$$

D.2 Möbius transformations

$$\frac{az+b}{cz+d}$$

D.3 The modular group

Define Möbius transformations

$$S = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$$
$$T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$$

As before, the actions of these two matrices are as follows:

$$Sz = \frac{0z+1}{-1z+0} = -\frac{1}{z}$$
$$Tz = \frac{1z+1}{0z+1} = z+1$$

S is an inversion about the unit circle ($z \mapsto 1/z$) followed by reflection across the imaginary axis ($z \mapsto -z$), while T is a simple translation.
These form a "basis", a generating set, for the modular group:

Proposition D.3.2. $\mathrm{PSL}_2(\mathbf{Z}) = \langle S, T \rangle$.

D.4 A fundamental domain for $\mathrm{PSL}_2(\mathbf{Z})$

Definition D.4.3. *Let* $F \subset \mathfrak{H}$ *be a closed set with connected interior, and let* Γ *be a subgroup of* $\mathrm{PSL}_2(\mathbf{Z})$*. We say* F *is a* fundamental domain *for* $\Gamma\backslash\mathfrak{H}$ *or for* Γ *if*

1. *any* $h \in \mathfrak{H}$ *is* Γ*-equivalent to some point in* F
2. *no two interior points of* F *are equivalent under the* Γ *action*
3. *the boundary of* F *is piecewise smooth*

Define $\mathbf{M} = \mathrm{PSL}_2(\mathbf{Z})$.
We now exhibit a fundamental domain for $\mathrm{PSL}_2(\mathbf{Z})$. Let

$$F = \{h \in \mathfrak{H} : |\mathfrak{R}(h)| \leqslant \frac{1}{2}, |h| \geqslant 1\}$$

Proposition D.4.4. F *is a fundamental domain for* $\mathbf{M}$.

D.5 Congruence subgroups

Definition D.5.5. *Let* $N \in \mathbf{Z}_{>0}$. *The* modular group *of* level N *is*

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{M} : c \equiv 0 \pmod{N} \right\}$$

We also have

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{M} : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$$

and the *principal congruence subgroups*

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{M} : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$$