Number theory and arithmetic geometry

Soham Chowdhury

August 9, 2017

Contents

I Basic notions **1**

1 Category theory **2**
1.1 Adjunctions . . . 2

2 Sheaves **3**

3 Affine schemes **4**
3.1 Motivation . . . 4
3.2 The spectrum of a ring . . . 4
3.3 Some examples . . . 5

4 Algebraic integers **6**
4.1 Appetizer: Fermat's theorem on sums of two squares . . . 6
4.2 Integral closure . . . 9
4.3 Integrality . . . 9
4.4 The trace and the norm . . . 10
4.5 Galois-theoretic interpretations . . . 10
4.6 Integral bases . . . 10

5 Valuations **12**

A Commutative algebra **13**
A.1 Rings . . . 13
A.2 Tensor products of modules . . . 13
A.3 Operations on modules . . . 13
A.4 Localization . . . 13

B Complex analysis **14**
B.1 Holomorphy and complex differentiability . . . 14
B.2 Power series . . . 17
B.3 Contour integration . . . 19
B.4 Zeroes and poles . . . 19

C Fourier analysis **20**
C.1 Fourier expansions . . . 20
C.2 Meromorphy . . . 20

D Modular forms **22**
D.1 The hyperbolic plane . . . 22
D.2 Möbius transformations . . . 22
D.3 The modular group . . . 22
D.4 A fundamental domain for $\mathrm{PSL}_2(\mathbf{Z})$ . . . 22
D.5 Congruence subgroups . . . 23

E Inequalities **24**

Part I

Basic notions

Chapter 1

Category theory

1.1 Adjunctions

Consider a pair of functors between C and D.

$$\begin{aligned} \mathsf{F}\colon \mathsf{C} &\to \mathsf{D} \\ \mathsf{C} &\leftarrow \mathsf{D}\colon \mathsf{G} \end{aligned}$$

An adjunction between C and D consists of natural transformations

$$\begin{aligned} \eta\colon 1_{\mathsf{C}} &\to \mathsf{G} \triangleleft \mathsf{F} \\ \mathsf{F} \triangleleft \mathsf{G} &\to 1_{\mathsf{D}}\colon \epsilon \end{aligned}$$

(called the *unit* η and the *counit* ϵ respectively)
Another definition states that F and G form an adjoint pair if there is an isomorphism

$$\mathsf{C}(\mathsf{G}Y, X) \simeq \mathsf{D}(Y, \mathsf{F}X)$$

natural in $X \in \mathsf{C}$ and $Y \in \mathsf{D}$.

Chapter 2

Sheaves

Chapter 3

Affine schemes

3.1 Motivation

The main objects of study in "modern" algebraic geometry are *schemes* – a certain kind of "geometric space" that encompasses both geometric questions (such as questions about lines on surfaces) and number-theoretic or arithmetic problems (such as questions about integral points on curves). This all works out because schemes are built from rings, so we can cast geometric problems in terms of rings of functions on geometric spaces – and algebraic number theory has been a thing for a very long time. This is a major idea behind algebraic geometry: sometimes it pays to look at some geometric object by considering the functions defined on that space.

For instance, given a topological space T , you can ask

Question 3.1.1. *What continuous real-valued functions* $f : T \to \mathbf{R}$ *can I define on the space, satisfying* P*?*

where P is some property of continuous $\mathbf{R}$-valued functions.

This question, by allowing you an indirect look at the space, often reveals very interesting information about the space that would have been difficult to gain otherwise. You can do similar things for smooth or complex manifolds. This "indirect viewpoint" is the primary one adopted in algebraic geometry.

Slogan 3.1.2. Instead of looking at a space, look at the (rings of) functions defined on its subsets.

Here is some motivation for what schemes are like, using some words we haven't defined here yet. You may have heard of differentiable or smooth manifolds: they are spaces that locally "look like" $\mathbf{R}^n$. For instance, a sphere looks like $\mathbf{R}^2$ if you "zoom in" enough. And we understand $\mathbf{R}^2$ just fine, and $\mathbf{R}^n$ in general – this is just multivariable calculus. The idea here is that we can work with complicated spaces as long as, "locally", they look like things we understand.

The definition we are aiming for is this:

Target Definition 3.1.3. *A scheme is a "locally ringed space" that is locally isomorphic to an affine scheme.*

We will now spend some time constructing the notions that go into that statement, building intuition for what these things *are*. In this chapter, we define *affine schemes*, which are to schemes what Euclidean spaces are to manifolds.

3.2 The spectrum of a ring

Provisional Definition 3.2.4. *Define the* spectrum *of a ring* R *as (at least for now) the set*

$$\operatorname{Spec} R = \{I \subseteq R : I \textit{ is a prime ideal}\}$$

The element of $\operatorname{Spec} R$ corresponding to the prime ideal P of R will be denoted $[P]$ when it is not clear from context.

3.3 Some examples

Example 3.3.5. The *ring of dual numbers* over the field k is written $k[\epsilon]/(\epsilon^2)$. Consider the associated affine scheme

$$X = \operatorname{Spec} k[\epsilon]/(\epsilon^2)$$

What are its points? This is equivalent to asking what its prime ideals are. Since $\epsilon^2 = 0$, $k[\epsilon]/(\epsilon^2)$ is not an integral domain and so (0) is not a prime ideal. Any other ideals will be generated by linear polynomials in ϵ, and one can try to reason further by considering generators of ideals in $k[\epsilon]/(\epsilon^2)$, which will be (monic) linear polynomials.

However, a quicker argument goes as follows: note that, by Proposition A.1.3, prime ideals of $k[\epsilon]/(\epsilon^2)$ are the same as prime ideals of $k[\epsilon]$ containing the ideal (ϵ^2). Since $k[\epsilon]$ is a PID, every prime ideal $\mathcal{P}$ is generated by some prime element p. So

$$(\epsilon^2) \subset (p) = \mathcal{P} \implies p \mid \epsilon^2$$

but the only prime element dividing ϵ^2 is ϵ, so $\mathcal{P} = (\epsilon)$. Hence the only point of the scheme X is that corresponding to (ϵ).
A

Chapter 4

Algebraic integers

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

4.1 Appetizer: Fermat's theorem on sums of two squares

Question 4.1.1. *Does the equation*

$$p = a^2 + b^2 \qquad (p \textit{ prime}) \tag{4.1}$$

have nontrivial solutions with integer a *and* b*?*

A bit of history This post is yet another from Ye Olde Days: I found a stray LaTeX file in an old `/home` folder. I wrote this for a friend at Canada/USA Mathcamp, as part of my usual Number Theory Indoctrination Service.

One start is to look at the equation mod 4. Since squares are always either 0 or 1 modulo 4 (work this out for yourself if it's not familiar) p can only be 1 mod 4. [1] Keeping this in mind, we restrict our attention to primes $\equiv 1 \pmod 4$.
We notice that a nontrivial "factorization" of p of the form

$$p = (a + ib)(a - ib) a, b \in \mathbf{Q}$$

gives us an expression of the form we want, if we are willing to expand our notion of what factorization means beyond its usual meaning in $\mathbf{Z}$. In fact, the approach that we follow is to look at how different primes factor or "split" in the ring $\mathbf{Z}[i]$, which is the ring of numbers of the form

$$\mathbf{Z}[i] = \{a + ib : a, b \in \mathbf{Z}\}$$

We will obtain a complete description of how integer primes split in this ring, the *ring of Gaussian integers*, and thus prove the following:

Theorem (Fermat)**.** *A prime number can be expressed as a sum of two integer squares iff it is congruent to* 1 *mod* 4*.*

$\mathbf{Z}[i]$ as a lattice

Notice that it can often be worthwhile to think of $\mathbf{Z}[i]$ geometrically, as a subset of the complex plane corresponding to all the complex numbers with integer real and complex parts. This gives $\mathbf{Z}[i]$ the structure of a (square) *lattice*, which has an obvious meaning that we will not work hard to rigorize for now: think of the points in the plane with integer coordinates, where (x, y) corresponds to $x + iy$.

[1] 0 and 2 are, uh, not really possibilities, except in the case $2 = 1^2 + 1^2$.

Aside 4.1.2. This has very deep applications once we start considering more interesting number fields: here we are looking at $\mathbf{Q}(i)$ and its *ring of integers* $\mathbf{Z}[i]$, and $\mathbf{Q}(i)$ is basically the nicest number field in existence. We will see that arguments using the "geometry of numbers", also called *Minkowski theory*, are very powerful, and will (for instance) enable us to prove the Dirichlet unit theorem.

Preliminaries

First, we review a few definitions from ring theory.
For example, 2 is not irred in $\mathbf{Z}[i]$, since $2 = (1+i)^2$, but it is an irred in $\mathbf{Z}$, since the only ways to write it as a product are silly things like $(-1)\cdot(-2)$ and -2 is manifestly a unit times 2.

Definition 4.1.3. A ring R is *Euclidean* if there exists a function

$$\nu : R \setminus \{0\} \to \mathbf{Z}^{\geqslant 0},$$

called the *Euclidean valuation*, such that we can perform a "division algorithm" in the ring using ν.

That is, for any $a, b \in R$, there exist $q, r \in R$ such that[2]

$$a = bq + r, \nu(r) < \nu(b).$$

For instance, $\mathbf{Z}$ is an Euclidean domain with valuation $\nu(r) = |r|$.

Definition 4.1.4. A *principal ideal domain*, or *PID* for short, is a ring where all ideals are generated by a single element (all ideals are *principal*).

Definition 4.1.5. A *unique factorization domain* (often *UFD* for short, or sometimes *factorial* ring or domain) is a ring where elements can be uniquely factored into irreducible elements. That is, for all $r \in R$, there exists a factorization

$$r = u \cdot p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where u is a unit, and the p_i and a_i are unique, up to reordering of the p_i.

Now, we have:

Theorem 4.1.6. *Euclidean domain $\implies$ PID.*

Proof. Consider an arbitrary ideal I of our ring R. Choose a smallest nonzero element w from I (where "smallest" refers to the valuation being the least).
Any other element of I can be written as

$$a = wq + r$$

where $\nu(r) < \nu(w)$. But there is no such nonzero element, by the assumption that w has the smallest valuation of any element of I. We conclude that $r = 0$. Hence w divides every other element of I, so $I = (w)$. ∎

Very Useful Theorem 4.1.7. *PID $\implies$ UFD.*

Proof. The proof is too messy to include here. Some references are provided in the margin. A quick google turned up this pdf. ProofWiki also has an incomplete proof. ∎

It's worth taking a moment to do the following (easy) exercise:

Exercise 4.1.A. In any integral domain, primes are irreducible.

There is, in fact, a very important partial converse:

Exercise 4.1.B (and Fact)**.** In a UFD, irreducibles are prime.

This will be helpful shortly. In fact, the only reason why we went to all the trouble with PIDs and so on is so that we could state this fact!

[2] Note that the valuation of 0 is not defined, at least per this definition. However, setting $\nu(0) = 0$ seems to work just fine.

$\mathbf{Z}[i]$ is a UFD

Proposition 4.1.8. *The function $\nu : \mathbf{Z}[i] \to \mathbf{Z}^{\geqslant 0}$ defined by*

$$\nu(a + ib) = a^2 + b^2 = |a + ib|^2$$

is an Euclidean valuation on the ring $\mathbf{Z}[i]$.

Proof. Given $a, b \in \mathbf{Z}[i]$, we need to show that there exist $q, r \in \mathbf{Z}[i]$ such that

$$a = bq + r \qquad\qquad |r|^2 < |b|^2 \tag{4.2}$$

This is equivalent to $\frac{a}{b} - q = \frac{r}{b}$.
We need to find a b such that

$$\left|\frac{a}{b} - q\right| = \left|\frac{r}{b}\right| < 1.$$

Why is this possible? Notice that the number $\frac{a}{b}$ lies in some square of the lattice formed by the Gaussian integers in the complex plane. So there will always be some lattice point within (at most) half the length of a diagonal of a lattice square from $\frac{a}{b}$. This suffices, since that length is $\frac{\sqrt{2}}{2} < 1$. ∎

If $p = 4n + 1$ is a prime, then the congruence

$$-1 \equiv x^2 \pmod{p}$$

has a solution: indeed, by Wilson's theorem,

$$\begin{aligned} -1 \equiv (p-1)! &= (1 \cdot 2 \cdots (2n)) \cdot ((2n+1) \cdot (2n+2) \cdots (4n)) && (4.3)\\ &\equiv (1 \cdot 2 \cdots (2n)) \cdot ((-2n) \cdot (-2n+1) \cdots (-1)) && (4.4)\\ &= (2n)! \cdot (-1)^{2n} (2n)! && (4.5)\\ &= [(2n)!]^2 \pmod{p} && (4.6) \end{aligned}$$

so taking $x = (2n)!$ works.
Now we are ready to prove the main theorem. We restate it here:

Theorem 4.1.9 (Fermat)**.** *A prime number can be expressed as a sum of two integer squares iff it is congruent to 1 mod 4.*

Proof. It now suffices to show that a prime $p \in \mathbf{Z}$ does not remain prime in $\mathbf{Z}[i]$ if $p \equiv 1 \pmod 4$. When that is done, we have a nontrivial factorization

$$p = \alpha \cdot \beta$$

and taking norms (i.e. valuations) of both sides gives

$$p^2 = (a^2 + b^2) \cdot \nu(\beta)$$

where we write $\alpha = a + ib$. Now, since the factorization is nontrivial, neither α nor β are units, and hence we have $p = a^2 + b^2$, and we're done.
But for primes congruent to 1 modulo 4, we have our lemma which states that there exists x such that $x^2 + 1 \equiv 0 \pmod 4$. So $p | x^2 + 1 = (x + i)(x - i)$, but it does not divide either of the factors on the right (it doesn't divide either of their imaginary parts). So p is not prime in $\mathbf{Z}[i]$.
Now we use all the algebra we did: since $\mathbf{Z}[i]$ is a UFD, our Fact from before tells us that p not prime implies that p is not irreducible. So p has some factorization

$$p = \alpha \cdot \beta$$

in $\mathbf{Z}[i]$, and we're done. ∎

4.2 Integral closure

4.3 Integrality

The setup

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

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \longrightarrow & B \end{array}$$

Basic properties

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

Proof. TODO. ∎

Corollary 4.3.11. *If* a *and* b *are integral over* A*, so are* $a + b$ *and* ab*.*

Theorem 4.3.12 (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 4.3.13. *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 4.3.14. 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 4.3.15. $l \in L$ *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 4.3.11, 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 $\mu \in A[x]$. ∎

4.4 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

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

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

Remark 4.4.16. If this isn't immediately clear, think Vietà. (This will be one of the recurring themes throughout this chapter.)

4.5 Galois-theoretic interpretations

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

Proposition 4.5.17. *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 4.5.18. *For a tower of finite extensions $K \subseteq L \subseteq M$, we have*

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

$\cos x$

4.6 Integral bases

Definition 4.6.19. 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 4.6.20. *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 4.6.21. *For $L\,|\,K$ and α_i as above,*

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

Proof. The form has matrix

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

with respect to the given basis. The nondegeneracy of the form, which we have from Proposition 4.6.20, is equivalent to the statement that $\det M \neq 0$, whence the claim follows. ■

Lemma 4.6.22. *Let (α_i) be a basis of $L \mid K$ contained in B, with $d = d(\alpha_1, \ldots, \alpha_n)$. Then*

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

Proposition 4.6.23. *If $L \mid K$ 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 4.6.24. *B admits an integral basis over A.*

Proposition 4.6.25. *Let $M \mid K$ and $N \mid K$ 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 $M \mid K$ and $(\beta_j)_{1 \leqslant j \leqslant n}$ of $N \mid K$ 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 4.6.26. *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.

Chapter 5

Valuations

Appendix A

Commutative algebra

A.1 Rings

Proposition A.1.1. *The preimage of a prime ideal is also a prime ideal: given a ring map* $\phi : A \to B$ *and a prime ideal* $I \subset B$, $\phi^{-1}(I) \subset A$ *is also prime.*

Proof. Let $J = \phi^{-1}(I)$, and consider $xy \in J$. Then $\phi(xy) = \phi(x)\phi(y) \in I$, so either $\phi(x) \in I$ or $\phi(y) \in I$, which in turn tells us that either $x \in J$ or $y \in J$. ■

Proposition A.1.2. *The surjective image of a prime ideal is also a prime ideal: given a surjective ring morphism* $\sigma : A \twoheadrightarrow B$ *and a prime ideal* $I \subset A$, $\sigma(I) \subset B$ *is also prime.*

Proof. This is a simple variant of the argument for Proposition A.1.1. Let $J = \sigma(I)$, and consider $xy \in J$. By surjectivity, there exist a and b such that

$$\sigma(a) = x$$
$$\sigma(b) = y$$

yielding $\sigma(ab) = xy$. Then $ab \in I$, which implies that (wlog) $a \in I$ since I is prime. Then $\sigma(a) = x \in J$, so that J is also prime. ■

Proposition A.1.3. *Let* I *be an ideal of* A*. Consider the natural map*

$$\pi : A \to A/I.$$

Then π^{-1} *gives an inclusion-preserving bijection between prime ideals of* A/I *and prime ideals of* A *containing* I*.*

Proof. This is one form of the third isomorphism theorem (TODO REF).

For one inclusion, we apply Proposition A.1.1, noting that (after convincing oneself that the map preserves inclusions) the preimage of a prime ideal $P \subset A/I$ must contain I since $(0) \subset P$ and $\pi^{-1}((0)) = I$. TODO ■

Proposition A.1.4. *The map* $\phi : k[x] \to k[x, \epsilon]/(\epsilon^2)$ *sending* $x \mapsto x + \epsilon$ *maps*

$$f(x) \mapsto f(x) + \epsilon f'(x).$$

A.2 Tensor products of modules

A.3 Operations on modules

A.4 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,

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

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

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

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

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

■

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 (Stokes' theorem-ish)**.** *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

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

Then we have the *Fourier expansion*

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

C.2 Meromorphy

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

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

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?

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

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

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

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

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

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

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

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*

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

Appendix E

Inequalities