Arithmetic geometry notes

Soham Chowdhury

July 23, 2017

Contents

Part I

Basic notions

Chapter 1

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*:

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

1.1 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 1.1.1 (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 1.1.2. *If* a *and* b *are integral over* A*, so are* $a + b$ *and* ab*.*

Theorem 1.1.3 (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 1.1.4. *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 1.1.5. 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 1.1.6. $l \in L$ *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 1.1.2, 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 $\mu \in A[x]$. ■

1.2 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

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

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

1.3 Galois-theoretic interpretations

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

Proposition 1.3.8. *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 1.3.9. *For a tower of finite extensions $K \subseteq L \subseteq M$, we have*

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

1.4 Integral bases

Definition 1.4.10. *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 1.4.11. *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 1.4.12. *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 1.4.11, is equivalent to the statement that $\det M \neq 0$, whence the claim follows. ■

Lemma 1.4.13. *Let* (α_i) *be a basis of* $L|K$ *contained in* B*, with* $d = d(\alpha_1, \dots, \alpha_n)$*. Then*

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

Proposition 1.4.14. *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 1.4.15. B *admits an integral basis over* A.

Proposition 1.4.16. *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 1.4.17. *If* $\mathfrak{i} \subseteq \mathfrak{j}$ *are two nonzero finite* $\mathscr{O}_K$*-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

Complex analysis

A.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 A.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 A.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 the Definition A.1.6.

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

This motivates the following definition.

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

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

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

$$\frac{\partial f}{\partial z}(a) = f'(a)$$
$$\frac{\partial f}{\partial \bar{z}}(a) = 0$$

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

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

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

are each equivalent to the following pair of equations:

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

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 A.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 A.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.

A.2 Zeroes and poles

Definition A.2.9 (Zeros)**.**

Definition A.2.10. *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 A.2.11 (Liouville)**.** *Any bounded entire function is constant.*

Definition A.2.12. *If* f *is holomorphic on all of* $\mathbf{C}$, *it is said to be* entire.

Appendix B

Fourier analysis

B.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*

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

B.2 Meromorphicity

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 C

Modular forms

C.1 The hyperbolic plane

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

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

C.2 Möbius transformations

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

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

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

Definition C.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

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

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

C.5 Congruence subgroups

Definition C.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*

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