Arithmetic geometry notes

Soham Chowdhury

July 18, 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

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

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 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 $d = d(\alpha_1, \ldots, \alpha_n)$. 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

In the definition of the derivative

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

take $h \in \mathbf{C}$. Write

$$\begin{aligned} f(z) \quad &= u(z) \quad + iv(z) \\ f(x,y) &= u(x,y) + iv(x,y) \end{aligned}$$

Then $f' = u_x + iv_x$, and similarly taking $h = ik$ gives $f' = v_y - iu_y$. Comparing the two expressions, we obtain the *Cauchy-Riemann equations*:

$$u_x = v_y \tag{A.1}$$

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

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

Definition A.1.1. *A function* $f : U \to \mathbf{C}$ *is* holomorphic, *or* complex differentiable, *if the limit*

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

exists. f *is said to be* holomorphic on U *if it is holomorphic at every point of* U.

Definition A.1.2. *If* f *is holomorphic on all of* $\mathbf{C}$, *it is said to be* entire.

From the explicit limits we calculated above, we know that holomorphy on a domain U implies that the Cauchy-Riemann equations hold on U. In fact, the converse is also true! Holomorphy is a much more rigid requirement than real-analytic differentibility on $\mathbf{R}^2$.

A.2 Zeroes and poles

Definition A.2.3 (Zeros).

Appendix B

Modular forms