Arithmetic geometry notes

Soham Chowdhury

July 17, 2017

Contents

Chapter 1

Algebraic integers

1.1 Integrality

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*:

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

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 $A[b_1, \dots, b_n]$ 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. $Tr_{L|K}(z) = \sum_\sigma \sigma z$
3. $Nm_{L|K}(z) = \prod_\sigma \sigma z$

Proof. Part 1 ■

Theorem 1.3.9. *Consider finite field extensions* $K \subseteq L \subseteq M$*. We have*

$$\begin{aligned} Tr_{L|K} \circ Tr_{M|L} &= Tr_{M|K} \\ Nm_{L|K} \circ Nm_{M|L} &= Nm_{M|K} \end{aligned}$$