Notes on Algebraic Number Theory

Ken Lee

Winter 2020

Goal : An account of algebraic number theory as geometric as possible, that is, as the study of the affine case of Noetherian smooth integral curves.

Contents

1 Dedekind Domains

1.1 Local Study

Definition – Noetherian, Integral, Krull Dimension

Let $X \in \mathbf{Aff}$ be an affine scheme.

- X is called *Noetherian* when any of the following equivalent conditions are met :
  1. $\mathcal{O}_X(X)$ is Noetherian.
  2. for all opens $U \subseteq X$, $\mathcal{O}_X(U)$ Noetherian.
  3. there exists an open cover $\mathcal{U}$ of X such that for all $U \in \mathcal{U}$, $\mathcal{O}_X(U)$ Noetherian.
- X is called *integral* when any of the following equivalent conditions are met :
  1. $\mathcal{O}_X(X)$ is an integral domain.
  2. the underlying topological space of X is irreducible and X is reduced.

– $\dim X :=$ Krull dimension of $\mathcal{O}_X(X)$. X is called a *curve* when $\dim X = 1$.

– Call X *local*[a] when any of the following equivalent definitions are met :

1. X has a unique closed point.
2. $\mathcal{O}_X(X)$ is a local ring.

– Let X be integral. Then X is *integrally closed* when any of the following equivalent definitions are met :

1. $\mathcal{O}_X(X)$ is integrally closed.
2. For all points $x \in X$, $[\mathcal{O}_X]_x$ is integrally closed.
3. For all closed points $x \in X$, $[\mathcal{O}_X]_x$ is integrally closed.

[a] I made this up.

Remark. Still no geometric intuition for integrally closed.

Proposition – Characterisation of DVRs

Let $X \in \mathbf{Aff}$ be a local Noetherian integral curve. Let p be its unique closed point and $\kappa(p)$ its residue field. Let $K := [\mathcal{O}_X]_{p_X}$ where p_X is the unique generic point of X, i.e. $K = \operatorname{Frac} \mathcal{O}_X(X)$. Then TFAE :

1. There exists a valuation $v : K^\times \to \mathbb{Z}$ with $\mathcal{O}_X(X)$ as its valuation ring.
2. $\mathcal{O}_X(X)$ is integrally closed.
3. $\ker \operatorname{ev}_p$ is principal.
4. $\dim_{\kappa(p)} T_p^* X = 1$, i.e. X is smooth.
5. The only ideals of $\mathcal{O}_X(X)$ are (0) and powers of $I(p)$. That is to say, the only closed subschemes of X are X and the infinitesimal neighbourhoods of p.
6. There exists $f \in \mathcal{O}_X(X)$ such that all non-zero ideals of $\mathcal{O}_X(X)$ are of the form (f^k) for some $k \in \mathbb{N}$.

$\mathcal{O}_X(X)$ is called a *discrete valuation ring* when any (and thus all) of the above are satisfied.

1.2 Global Definition

Proposition – Characterisation of Dedekind Domains

Let $X \in \mathbf{Aff}$ be integral but not a point. Then TFAE :

1. All non-zero $f \in \mathcal{O}_X(X)$ vanish at finitely many points and for all points $p \in X$, $[\mathcal{O}_X]_p$ DVR.
2. X is a Noetherian, integrally closed curve.
3. X is Noetherian curve and all primary ideals of $\mathcal{O}_X(X)$ is a power of a prime ideal.
4. X is a curve and for all non-zero ideals $I \subsetneq \mathcal{O}_X(X)$, I factorises into powers of prime ideals. i.e. All closed subschemes of X look like finitely many infinitesimal neighbourhoods of

points.

$\mathcal{O}_X(X)$ is called a *Dedekind domain* when any (and thus all) of the above are satisfied.

Furthermore, the factorisation in (4) turns out to be unique.

Proof. $(1 \Rightarrow 2)$ X integrally closed since being integrally closed is a stalk-local property. Stalk-local dimension 1 also easily implies global dimension 1. It remains to prove Noetherian.

Let $0 \neq I$ be an ideal of $\mathcal{O}(X)$. The unit case is clear so let $I \neq (1)$. There exists $0 \neq f \in I$. The key is that $V(I) \subseteq V(f)$ which is finite and at the stalks of each $p \in V(f)$, $I_p = g_p A_p$ for some $g_p \in I_p$. WLOG each g_p comes from I. The claim is that $I = Af + \sum_{p \in V(f)} Ag_p$. It suffices to check stalk-locally. This is clear by doing cases on $p \in V(f)$ or not.

$(2 \Rightarrow 3)$ Let I be a primary ideal of $\mathcal{O}_X(X)$. Since X is a curve, $V(I) = \overline{\{p\}} = \{p\}$ for some closed point $p \in X$. It is straightforward to show that $[\mathcal{O}_X]_p$ is a Noetherian, integrally closed, integral domain and hence a DVR. So there exists $N \in \mathbb{N}$, $I(p)_p^N = I_p$. It suffices to show $I(p)^N = I$. It suffices that for all points $q \in X$, $(I/I(p)^N)_q = 0$. But since X is a curve and $\operatorname{supp} A/I = V(I) = \{p\}$, it suffices to check for the point p, which we have already.

$(3 \Rightarrow 4)$ $\mathcal{O}_X(X)$ Noetherian implies all non-zero proper ideals have a primary decomposition. By assumption and X being a curve, primary ideals are powers of maximal ideals. Since powers of distinct maximal ideals are comaximal, a primary decomposition is the same as a factorisation into prime powers.

$(4 \Rightarrow 1)$ Non-zero global functions f vanish at finitely many points because all closed subschemes contain only finitely many points. Now let $p \in X$ be a closed point. It is clear that $[\mathcal{O}_X]_p$ is local and dimension 1. We show that non-zero proper ideals of $[\mathcal{O}_X]_p$ are powers of $I(p)_p$, which proves $[\mathcal{O}_X]_p$ is not only Noetherian but also a DVR. Well, any non-zero ideal of $[\mathcal{O}_X]_p$ must be of the form I_p for some non-zero proper ideal I of $\mathcal{O}_X(X)$. But I factorises into prime powers and since X is a curve, going to the stalk over p inverts any factors that aren't powers of $I(p)$, so I_p is a power of $I(p)_p$.

(*uniqueness of the factorisation*) Note that the primes occuring in any factorisation of an ideal I corresponds to the points in $V(I)$, so it suffices to check uniqueness of powers. Let $I(p_1)^{n_1} \cdots I(p_k)^{n_k} = I(p_1)^{m_1} \cdots I(p_k)^{m_k}$ where $p_1, \dots, p_k$ are distinct points. Since X is a curve, we can apply chinese remainder theorem to quotienting out $I(p_1)^{n_1} \cdots I(p_k)^{n_k}$ and realise the only ideals in each component are the prime powers. The isomorphism given by CRT preserves powers of ideals, to we must have $m_1 = n_1, \dots, m_k = n_k$.

□

1.3 Integral Closure of Dedekind Domains

Remark – Results of this section.

- Basic Properties of Trace and Norm
- Trace Characterisation of Finite Separable Extensions
- (Main) Integral Closure of Dedekind Domain in Finite Extension is Dedekind.

I reluctantly wrote about the trace and norm since it looks like ANT cannot theoretically do without them, but I still do not have geometric intuition for them.

Proposition – Trace Characterisation of Finite Separable Extensions
Let $K \to L$ be a finite extension. Then it is separable if and only if the bilinear form $L \times L \to K, \alpha, \beta \to \mathrm{Tr}(\alpha\beta)$ is non-degenerate.

Proof. (From Janusz) Don't want to think about trivial case of $K = L$, so we assume $K \to L$ is a non-trivial extension.

($\Rightarrow$) We use a clever K-basis of L to link the determinant of the trace form and separability of L over K. The clever basis is : let $L = K \oplus K\theta \oplus \cdots \oplus K\theta^{[L:K]-1}$ by the primitive element theorem so that given a finite Galois extension $K \to \Omega$ with $K\mathbf{Alg}(L, \Omega) = \left\{\sigma_1, \ldots, \sigma_{[L:K]}\right\} \neq \varnothing$, it suffices

$$\det\left[\mathrm{Tr}_{L/K}(\theta^{i-1}\theta^{j-1})\right] = \prod_{i<j}\left(\sigma_i(\theta) - \sigma_j(\theta)\right)^2$$

since the latter is non-zero by separability of L over K.

So let $K \to \Omega$ be a finite Galois extension with $K\mathbf{Alg}(L, \Omega) = \left\{\sigma_1, \ldots, \sigma_{[L:K]}\right\} \neq \varnothing$. Then we have the algebraic trick called the Vandermonde matrix :

$$\det\begin{bmatrix} 1 & & 1 \\ \sigma_1(\theta) & & \sigma_{[L:K]}(\theta) \\ \vdots & \cdots & \vdots \\ \sigma_1(\theta)^{[L:K]-1} & & \sigma_{[L:K]}(\theta)^{[L:K]-1} \end{bmatrix} = \prod_{i<j}\left(\sigma_i(\theta) - \sigma_j(\theta)\right)$$

So it suffices that $\left[\mathrm{Tr}_{L/K}(\theta^{i-1}\theta^{j-1})\right] = VV^t$. We have

$$[VV^t]_{i,j} = \sum_k \sigma_k(\theta^{i-1})\sigma_k(\theta^{j-1}) = \sum_k \sigma_k(\theta^{i-1}\theta^{j-1})$$

So it suffices that for any θ^l, the trace $\mathrm{Tr}_{L/K}(\theta^l) = \sum_k \sigma_k(\theta^l)$ in Ω. To see this for $l = 1$, note that $\mathrm{Char}(\theta, K) = \min(\theta, K)$ since the former has θ as a root and has the same degree as the latter. To get arbitrary l, note that $\mathrm{Char}(\theta, K) = \min(\theta, K)$ separable implies $[\theta]$ is diagonalisable in Ω with eigenvalues $\sigma_1(\theta), \ldots, \sigma_{[L:K]}(\theta)$. It follows that $[\theta^l]$ is diagonalisable in Ω as well, with eigenvalues $\sigma_1(\theta^l), \ldots, \sigma_{[L:K]}(\theta^l)$.

($\Leftarrow$) Suppose L is inseparable over K, so we have characteristic of K being some prime $p > 0$, $K \to L_S \to L$ where $K \to L_S$ is separable and $L_S \to L$ is purely inseparable with degree p^N for some $N > 0$. We need to give an $x \in L$ such that for all $y \in L$, $\mathrm{Tr}_{L/K}(xy) = 0$ but $x \neq 0$. By assumption, we have an $x \in L \setminus L_S$. Then for $y \in L$, $\mathrm{Tr}_{L/K}(xy) = \mathrm{Tr}_{L_S/K}\left(\mathrm{Tr}_{L/L_S}(xy)\right)$ so it suffices $\mathrm{Tr}_{L/L_S}(xy) = 0$. Well, if $xy \in L_S$, then $\mathrm{Tr}_{L/L_S}(xy) = p^N xy = 0$. If $xy \notin L_S$, then there exists $n > 0$ such that $\min(xy, L_S) = T^{p^n} - a$ for some $a \in L_S$. By working in an extension $L \to \Omega$ where $\mathrm{Char}(xy, L_S)$ splits, one sees that $\mathrm{Char}(xy, L_S)(T) = (T - xy)^{p^N}$ in Ω, and so $\mathrm{Char}(xy, L_S)(T) = (T^{p^n} - a)^{p^{N-n}}$, which implies $\mathrm{Tr}_{L/L_S}(xy) = 0$ again.

□

Proposition – Integral Closure of Dedekind Domain in Finite Extension
Let A be a Dedekind domain, K its field of fractions, $K \to L$ a finite extension of fields, B the

integral closure of A in L. Then B is a Dedekind domain.

Proof. (Milne, Janusz combined)

(*Integrally closed*) Transitivity of being integral over a base ring.

(*Dimension 1*) Let $q \in \operatorname{Spec} B$ be non-generic and $\pi : \operatorname{Spec} B \to \operatorname{Spec} A$ the adjunct of $A \to B$. Let $p = \pi(q)$. Then $0 \to A/I(p) \to B/I(q)$ is an integral extension of integral domains.

> *Lemma. For $A \subseteq B$ ID where B is integral over A, B is a field if and only if A is.*
>
> *Proof.* Atiyah. The argument is elementary. ■

So it suffices to prove p is not the generic point of $\operatorname{Spec} A$. Well, there exists $f \in B \setminus 0$ that vanishes at q. Since B integral over A, $f^n + a_1 f^{n-1} + \cdots + a_0 = 0$ for some $a_k \in A$. Let n be minimal. Then $0 \neq a_0 \in I(p)$.

(*Noetherian*) We have the decomposition $K \to L_{sep} \to L$ where $K \to L_{sep}$ is separable and $L_{sep} \to L$ is purely inseparable. We hence also have a decomposition $A \to A_{sep} \to B$ where A_{sep} be the integral closure of A in L_{sep} and it follows that B is the integral closure of A_{sep} in L. It thus suffices that B is Noetherian over A_{sep} and A_{sep} is Noetherian over A.

We first prove A_{sep} Noetherian over A by proving a more detailed lemma which gives us extra data for the example of algebraic integers.

> *Lemma. Let A be an integrally closed domain, $K \to L$ a finite separable field extension where K is the fraction field of A and B the integral closure of A in L. Then there exists free sub-A-modules $M, M_1 \subseteq L$ with rank $[L : K]$ such that $M \subseteq B \subseteq M_1$.*
>
> *In particular, A Noetherian implies B is Noetherian. Also, A PID implies B is also a free A-module with rank $[L : K]$.*
>
> *Proof.* Let $L = K\beta_1 \oplus \cdots \oplus K\beta_{[L:K]}$. For any $x \in L$, there exists $a \in A \setminus 0$ such that $ax \in B$. So we can WLOG assume $\beta_1, \ldots, \beta_{[L:K]} \in B$. Set $M := A\beta_1 + \cdots + A\beta_{[L:K]}$. Since $K \to L$ is finite separable, non-degeneracy of the trace form gives another K-basis $\beta'_1, \ldots, \beta'_{[L:K]}$ of L that is dual to the previous basis with respect to the trace form, i.e. $\operatorname{Tr}_{L/K}(\beta_i \beta'_j) = \delta_{i,j}$. Let $M_1 := A\beta'_1 + \cdots + A\beta'_{[L:K]}$. It remains to show $B \subseteq M_1$. Let $b \in B$. Then $b = \sum_i \lambda_i \beta'_i$ for some $\lambda_i \in K$. Then $\lambda_j = \operatorname{Tr}_{L/K}(b\beta_j) \in \operatorname{Tr}_{L/K} B \subseteq A$ by the two bases being dual w.r.t. the trace form. ■

So we have A_{sep} is a Dedekind domain.

Now we prove B is Noetherian over A_{sep}. According to Janusz, this is quite hard so we directly show B is Dedekind by showing all non-zero functions have finite vanishing and all stalks are DVRs. TODO.

□

2 Morphisms

2.1 Dominant Morphisms

Proposition – Characterisation of Dominant Morphisms

Let $\varphi^* : A \to B$ be an ring morphism where A, B are domains but not points. Then TFAE :

1. φ has dense image.
2. φ maps the generic point to generic point.
3. φ^* is injective.

φ is called *dominant* when it satisfies any (and thus all) of the above.

If φ^* is integral, then TFAAE :

4. φ surjective.

2.2 Ramified Points

2.3 Inertia Degree