COMPLETE DISCRETE VALUATION RINGS

HOJIN LEE

Abstract. This is an exposition on some basic properties of complete discrete valuation rings.

Contents

1. Preliminaries

We provide basic definitions and first properties.

Definition 1.1 (Discrete Valuation Rings)**.** A commutative ring A is called a discrete valuation ring (DVR) if it is a PID, and it has a unique nonzero prime ideal, denoted $\mathfrak{m}_A$. A generator of this unique nonzero prime ideal is called a uniformizer, and the field $\kappa_A := A/\mathfrak{m}_A$ is called the residue field.

Definition 1.2. A Dedekind domain is an integrally closed noetherian domain of dimension 1.[1]

Proposition 1.3. *A ring is a DVR if and only if it is a local Dedekind domain.*

Proof. Let A be a DVR; the only nontrivial part is showing that A is integrally closed. We will use the discrete valuation v which will be defined in a moment. Let x be an element in its fraction field that is integral over A. Then it must satisfy a relation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. As $v(x^n) = v(-a_{n-1}x^{n-1} - \cdots - a_0)$, in particular we must have $v(x^n) \geq v(-a_i x^i)$ for some $i < n$. As $v(-a_i x^i) = v(-a_i) + v(x^i) \geq v(x^i)$, we have $(n-i)v(x) \geq 0$, and as $n - i > 0$ we have $v(x) \geq 0$. So indeed $x \in A$, and A is integrally closed.

Conversely suppose A is a local Dedekind domain. The nontrivial part is showing that A is a PID. The maximal ideal $\mathfrak{m}$ must be principal ([1], Prop. 9.2.) but then if I is a nonzero proper ideal, it must have a prime ideal factorization, but since the only prime is $\mathfrak{m}$ we have $I = \mathfrak{m}^n$ for some n. As $\mathfrak{m}$ is principal, it follows that every ideal of A is principal, so A is a PID. □

DVRs are Dedekind domains, in particular. Now suppose A is a DVR, with uniformizer π. Every nonzero element of A can be written uniquely as $\pi^n u$ for $n \in \mathbb{N}$ and $u \in A^\times$; define a function $v : A \setminus 0 \to \mathbb{N}$ as $v(x) = n$. This is called the *valuation* of the DVR A. If $K = \operatorname{Frac} A$, then we can extend v to $K^\times \to \mathbb{Z}$, as any nonzero element of K is uniquely written in the form $\pi^n u$ for $n \in \mathbb{Z}$. We define another function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ on K by sending 0 to 0, and nonzero x to $c^{v(x)}$ with $0 < c < 1$, and note that this defines an *absolute value* on K; although there is an ambiguity on the choice of c, all such choices give rise to equivalent absolute values, hence the notion of completeness is unambiguous.

Definition 1.4 (Absolute values on fields)**.** An absolute value on a field K is a function $|\cdot|_K : K \to \mathbb{R}_{\geq 0}$ such that

(1) $|x| = 0$ if and only if $x = 0$;
(2) $|xy| = |x||y|$;
(3) $|x + y| \leq |x| + |y|$.

Date: November 7, 2025.

[1] In [6], the condition is weakened to having dimension ≤ 1.

It is indeed straightforward to check these for the absolute value defined on the fraction field of A induced by the valuation. When A is a DVR, we will always assume that the fraction field K inherits the absolute value structure defined as above. Note that in particular, absolute values define a metric space structure on K, and since A is naturally a subspace of K, it also inherits the same absolute value and metric structure. Also notice that A is precisely the set of K that has absolute value ≤ 1 regardless of the choice of c; if $k \in K$ has $|k| \leq 1$, this means that $c^{v(k)} \leq 1$, i.e., $v(k) \geq 0$ so $k \in A$. Absolute values also endow K with a natural structure of a metric space with $d(x, y) := |x - y|_K$.

Definition 1.5 (Complete DVRs)**.** Let A and K be as above. We call A a complete DVR if it is complete w.r.t. the metric space structure induced by the absolute value on K.

Example 1.6. The p-adic integers $\mathbb{Z}_p$ is a complete DVR with uniformizer p and residue field $\mathbb{F}_p$. Given any DVR A, the completion $\varprojlim A/\mathfrak{m}^n$ is a complete DVR.

Note that if A is a complete DVR, then its fraction field is also complete under the absolute value induced by A. Let $(a_n) \in K$ be a Cauchy sequence; find some N such that $n, m \geq N$ implies $|a_n - a_m| \leq 1$. In particular this means that $|a_n - k| \leq 1$ for some k and all $n \geq N$, i.e., $(a_n - k)$ is (eventually) a sequence in A. This sequence is again Cauchy, but as A was assumed to be complete this sequence must converge to some limit in A. Hence the original sequence also converges, so K is complete.

Definition 1.7 (Norms)**.** Let V be a vector space over a field K equipped with an absolute value $|\cdot|_K$. A norm on V is a function $||\cdot|| : V \to \mathbb{R}_{\geq 0}$ such that

(1) $||v|| = 0$ if and only if $v = 0$;
(2) $||\lambda v|| = |\lambda|_K ||v||$ for every $\lambda \in K$ and $v \in V$;
(3) $||v + w|| \leq ||v|| + ||w||$ for every $v, w \in V$.

In particular, if we view a field extension L/K as a vector space L over K, then an absolute value on the field L naturally restricts to a norm on L as a K-vector space. We will need this later.

2. Integrally Closed Finite Extensions of Complete DVRs are Complete DVRs

We want to prove the following statement:

Any finite ring extension of a complete discrete valuation ring is again a complete discrete valuation ring.

We will try to remove ambiguity of this statement. It would've been convenient to fix our setup to where A is a complete DVR, K is its fraction field, L/K is a finite extension of fields[2] and B is the integral closure of A in L, and then show that B is a complete DVR. But I wanted to make sure to prove the statement with a minimal amount of assumptions, so I added them one-by-one until the statement had no counterexamples and was provable. In fact, as we will see below it turned out that the setup above is indeed minimal. Recall the definition of a finite ring extension:

Definition 2.1 (Finite ring extensions)**.** Let $A \subset B$ be an inclusion of commutative rings. We say that B is a finite ring extension of A, if B is finitely generated as an A-module via the structure induced by the inclusion. We omit the term *ring* when the context is clear.

Now here is a silly counterexample when we have no additional assumption on the ring B. Take your favorite complete DVR, say $\mathbb{Z}_p$, and consider the diagonal embedding $\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p \times \mathbb{Z}_p$ which is a ring extension. The $\mathbb{Z}_p$-module structure induced by this inclusion coincides with the usual $\mathbb{Z}_p$-module structure on the direct sum $\mathbb{Z}_p \oplus \mathbb{Z}_p$, which is obviously a finitely generated $\mathbb{Z}_p$-module. But the product ring isn't even a domain. We don't want this, so let us add that as an assumption and see what happens. A first guess is that there still are counterexamples (i.e., non-integrally closed cases) as in the number field case, such as $\mathbb{Z} \subset \mathbb{Z}[\sqrt{5}] \neq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. This is indeed true; in fact, we can *localize* this example as follows:

Proposition 2.2. *There exists $A \subset B$ where A is a complete DVR and B is an integral domain which is a finite ring extension of A, but is not integrally closed, hence is not a DVR.*

[2] We do *not* assume that L/K is separable, although we will need it in the next section.

Proof. Let $A = \mathbb{Z}_2$, and let $B = \mathbb{Z}_2[\sqrt{5}]$. The number 5 is not a 2-adic square; if you mod out by 8, the only odd square is 1. So this extension is nontrivial. Its fraction field is $\mathbb{Q}_2(\sqrt{5})$; consider the element $\alpha = \frac{1+\sqrt{5}}{2}$. This satisfies the monic equation $\alpha^2 - \alpha - 1 = 0$ but is obviously not contained in B, as 2 is not invertible. So B is not integrally closed, hence not a DVR. □

So we have to add the condition that the bigger ring is integrally closed. Say, A is a complete DVR, $A \subset B$ is a finite extension where B is an integrally closed domain. In this case, we obtain a familiar setting; let $K = \operatorname{Frac} A$ and $L = \operatorname{Frac} B$.

Lemma 2.3. $[L : K] < \infty$.

Proof. As $A \subset B$ is finite, we may write $B = A[b_1, \dots, b_n]$ for $b_i \in B$ integral over A. Note that $K(b_1, \dots, b_n) \subset L$, which is immediate. But $K(b_1, \dots, b_n)$ contains B, and is a field, hence must contain L. So in fact $L = K(b_1, \dots, b_n)$, and as b_i were integral over A, in particular they are algebraic over K and hence $[L : K]$ is finite. □

Lemma 2.4. *B is the integral closure of A inside L.*

Proof. Denote as $\widetilde{A}$ the integral closure of A inside L. As B was finite over A, its elements are integral over A. So $B \subset \widetilde{A}$. Conversely, let $x \in \widetilde{A}$. This means that $x \in L$ is integral over A; as $A \subset B$ this automatically implies that x is integral over B. But B is integrally closed, so $x \in B$. Therefore $\widetilde{A} = B$. □

So it is indeed reasonable to assume that we are given a complete DVR A, a finite extension L/K of its fraction field K, and B the integral closure of A inside L. We will first prove a preliminary result:

Lemma 2.5. *Let A, B, K, L be as assumed, together with the assumption that $A \subset B$ is finite. Then B is a Dedekind domain.*

Proof. By assumption, B is integrally closed. Also $\dim B = \dim A = 1$ as $A \subset B$ is integral. (You can prove this using the Cohen-Seidenberg theorems a.k.a. going-up, lying-over and incomparability.) The fact that B is a noetherian ring follows from finiteness of $A \subset B$, Hilbert's basis theorem, and the fact that quotients of noetherian rings are noetherian. So B is indeed a Dedekind domain. □

Theorem 2.6 ([8], Theorem 10.1[3])**.** *Let A, B, K, L be as in 2.5. Denote as $\mathfrak{m}_A$ the unique nonzero prime ideal of A. Then B is a DVR with its unique nonzero prime ideal $\mathfrak{m}_B$ lying over $\mathfrak{m}_A$.*

Proof. Consider the ideal $\mathfrak{m}_A B$; this is proper in B (otherwise, π_A^{-1} would be integral over A but this is absurd) and hence must have a factorization into nonzero prime ideals of B, as B is Dedekind by 2.5. So there is at least one nonzero prime ideal lying over $\mathfrak{m}_A$. Assume by contradiction that we have two distinct $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spm} B$ lying over $\mathfrak{m}_A$. W.l.o.g. we may choose $b \in \mathfrak{p} \setminus \mathfrak{q}$, and consider the ring $A[b] \subset B$. Note that $\mathfrak{p} \cap A[b]$ and $\mathfrak{q} \cap A[b]$ are distinct prime ideals of $A[b]$. They are distinct as one contains b while the other doesn't, and it is straightforward to check that both are prime ideals. By assumption they both are nonzero, and as $A \subset A[b]$ is integral ($b \in B$ is integral over A) we have $\dim A[b] = \dim A = 1$. So in fact $\mathfrak{p} \cap A[b]$ and $\mathfrak{q} \cap A[b]$ are distinct maximal ideals of $A[b]$ lying over $\mathfrak{m}_A$.

Now let $f \in K[x]$ be the minimal polynomial of b over K; as A is integrally closed, such f is actually in $A[x]$. Consider the image $\overline{f}$ in the ring $\kappa_A[x]$. As $\kappa_A[x]/(\overline{f}) \cong A[x]/(\mathfrak{m}_A, f) \cong A[b]/\mathfrak{m}_A A[b]$, and since there were two distinct maximal ideals of $A[b]$ lying over $\mathfrak{m}_A$ (i.e., containing $\mathfrak{m}_A A[b]$) we may conclude that $(\overline{f})$ is contained in two distinct maximal ideals of $\kappa_A[x]$, say (a) and (b). (Polynomial rings over fields are PIDs.) In particular this means that $\overline{f}$ contains two non-associate irreducible factors, so we can write $\overline{f} = \overline{g}\overline{h}$ for $(\overline{g}, \overline{h}) = (1)$. Now since A is a *complete* DVR, by Hensel's Lemma ([5] II.4.6.) this lifts to a nontrivial factorization $f = gh \in A[x]$ which contradicts the irreducibility of f. So in fact there can only be one prime ideal of B lying over $\mathfrak{m}_A$.

As $A \subset B$ is integral, maximal ideals downstairs correspond to maximal ideals upstairs, so every maximal ideal of B (i.e., every nonzero prime ideal) must lie over $\mathfrak{m}_A$. But we've shown that there is one, and there can only be one. So B has exactly one nonzero prime ideal, and by 1.3 this means that B is a DVR. □

[3]The proof in [8] assumes L/K is separable, but our argument holds without this assumption, provided $A \subset B$ is finite.

So we've seen that in our setup, B becomes a DVR. Now we show the completeness of B. The idea is that we will show that a suitable choice of an absolute value $|\cdot|_L$ induced by the valuation of B actually extends $|\cdot|_K$, and hence defines a norm of L as a K-vector space. This turns out to be complete via the discussion below.[4] The statement is slightly modified into a more pragmatic form.

Lemma 2.7 ([2], I.§2 Theorem 2)**.** *Let K be as above. Every n-dimensional Hausdorff topological vector space over K is isomorphic to K^n equipped with the product topology, as topological vector spaces.*

Caution: In general, topological vector spaces do not come with a metric. As completeness is a metric property (i.e., *not* preserved by homeomorphism) there are some technicalities; we will use without proof the fact that "completeness of TVSs" (not defined here, see [4] for details on Cauchy nets) is equivalent to metric completeness in our case of interest, and furthermore that TVS isomorphisms preserve completeness. (See [3].)

Corollary 2.8. *Let V be a finite dimensional vector space over a complete field K equipped with a norm compatible with the absolute value on K. Then V is complete.*

Proof. Let V be an n-dimensional normed vector space over K. Then by 2.7 it follows that the underlying TVS structure of V is isomorphic to K^n equipped with the product topology. Note that the normed space $(K^n, ||\cdot||_{\text{sup}})$ has an underlying TVS structure the same as the product topology (the K-linear structure is obviously the same). As this normed space is clearly complete (basically boils down to K being complete) it follows that its underlying TVS is also complete. Since completeness of TVS is preserved under isomorphism of TVSs, the TVS underlying the normed space V is complete. This implies V is complete as a normed space, in particular. $\square$

Here is the diagram of the situation above, for a better understanding:

$$\begin{tikzcd}
\text{Normed Spaces} & (K^n, ||\cdot||_{\text{sup}}) \arrow[d, dash, "\text{underlies}"] & (V, ||\cdot||) \arrow[d, dash, "\text{underlies}"] \\
\text{Topological Vector Spaces} & (K^n, \pi) \arrow[r, dash, "\sim"] & (V, \tau)
\end{tikzcd}$$

The symbols π and τ denote the respective topologies. Note that in [6] the fact that B has a unique nonzero prime (2.6) is proven using the fact that there can be only one norm on L, which follows from the fact that the topological vector space structure is unique.

Theorem 2.9. *Let A, B, K, L be as in 2.5. Then L is complete w.r.t. its absolute value induced by B. In particular, B is complete.*

Proof. Denote by $|\cdot|_L$ the absolute value defined on L via the discrete valuation (2.6) of B. Denote by π_A and π_B the respective uniformizers, and denote by v_A and v_B the respective discrete valuations. As $\pi_A B = (\pi_B)$, we have $\pi_A \in (\pi_B)$, i.e., $\pi_A = b\pi_B$ for some $b \in B$, where since $b = u\pi_B^k$ uniquely, we have $\pi_A = u\pi_B^e$ for $u \in B^\times$ and $e > 0$. Suppose the absolute value on K is given by $|x|_K = c^{v_A(x)}$; we define $|x|_L$ to be $c^{v_B(x)/e}$. We want to show that this $|\cdot|_L$ extends $|\cdot|_K$, i.e., they agree on K. Suppose $x \in K$; then we can write $x = v\pi_A^n$ uniquely where v is a quotient of units in A. Hence we have $|x|_K = c^n$. Now as $\pi_A = u\pi_B^e$, we have $x = vu^n\pi_B^{en}$ where vu^n is a quotient of units of B. Thus it follows that $|x|_L = c^{v_B(x)/e} = c^n$, which is $|x|_K$. Since $|\cdot|_L$ is an absolute value on L that restricts to $|\cdot|_K$ on K, it naturally defines a norm on L as a K-vector space. By 2.8 the norm must be complete, hence L together with its absolute value is a complete metric space. As $B = \{x \in L \mid |x|_L \le 1\}$, it is a closed subspace of L, hence complete.

$\square$

3. Discriminants

Now furthermore assume that L/K is a finite *separable* field extension. Separability is essential in this section, unlike the previous one. Denote by B the integral closure of A in L; in this case, B is finite over A by [6], I.§4 Prop. 8, and the field of fractions of B is indeed L by its preceding remark. Hence by our discussion

[4]In [6], the discussion of 2.8 and 2.9 is simplified into the words "As K is complete, so is K^n, hence L." This statement needs clarification; there is no metric of K^n specified in the book, only its topology, and there needs to be some discussion on the fact that completeness can be well defined for topological vector spaces even without a choice of a metric.

above we see that B is also a complete DVR, and we obtain our familiar setup, together with the additional assumption that L/K is separable. If we denote the respective uniformizers as π_A, π_B, then as we have seen in 2.9 we obtain a ramification index $\pi_A = u\pi_B^e$ for $e > 0$. Also denote the respective residue fields as κ_A and κ_B. We will first see that κ_B is a field extension of κ_A; consider the composition $A \to B \to B/(\pi_B)$ where the maps are the obvious ones. If $a \in (\pi_A)$, then as $\pi_A B = (\pi_B)$ we have $a \in (\pi_B)$. This means that (π_A) is sent to zero under this map, so it factors to $\kappa_A \to \kappa_B$ which is a field homomorphism, i.e., a field extension.

Definition 3.1. The extension L/K is unramified if $e = 1$ and κ_B/κ_A is separable.

Before proving anything, recall some familiar definitions:

Definition 3.2 (Trace pairing)**.** Let L/K be a finite extension. Define a function $\mathrm{Tr}_{L/K} : L \to K$ by taking the trace of the K-linear map $\mathrm{mult}_x : L \to L$, for $x \in L$. This is an additive group homomorphism. The K-bilinear form on L defined by $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is called the trace form. This definition naturally extends to the case where L is a finite commutative K-algebra, not necessarily a field. We will need this later.

In fact, the trace form Tr defined on fields is nondegenerate if and only if L/K is separable.

Proposition 3.3 ([7], Lemma 9.20.7)**.** *Let L/K be a finite extension and consider the trace pairing $\mathrm{Tr}_{L/K}$. This pairing is nondegenerate if and only if L/K is a separable extension.*

Proof. Suppose L/K is separable. By the Primitive Element Theorem we may write $L = K(\alpha)$ for some $\alpha \in L$. Note that the minimal polynomial m_α of α is identical to the characteristic polynomial P, say $x^d + a_1x^{d-1} + \cdots + a_d$ where $d = [L : K]$, as the extension is simple. This P has d distinct roots, say $\alpha_1, \ldots, \alpha_d$, in an algebraic closure $\overline{K}$ of K, as α was separable. These are the eigenvalues of α; so the trace of α^e is equal to $\alpha_1^e + \cdots + \alpha_d^e$. This sum is nonzero for some e large enough, by linear independence of the characters $\mathbb{Z} \to \overline{K}^\times$. This means that the trace of α^e is nonzero; if we have another nonzero element $\gamma \in L$, then $\mathrm{Tr}_{L/K}(\gamma, \alpha^e/\gamma) \neq 0$ so the pairing cannot be degenerate.

Conversely, suppose the extension L/K is not separable. We may decompose this as $L/K'/K$ where L/K' is a purely inseparable extension of degree p. By transitivity of trace, it suffices to show that such extensions have degenerate trace form. In that case, we have $L = K'(\alpha)$ with $\alpha^p \in K$; obviously $\mathrm{Tr}_{L/K'} = 0$ and for α^i, $i > 0$, the minimal polynomial for α^i over K is equal to $x^p - \alpha^{pi}$, and as the trace equals the $p-1$th term this must be zero. As the α^i for $0 \leq i < p$ form a K'-basis of L, the trace form is identically zero on L and is degenerate. □

Note that as B is a finite extension of a PID our discussion below is very similar to that of $\mathbb{Z}$.

Definition 3.4 (Discriminant)**.** For elements $e_1, \ldots, e_n$ of L, denote $\mathrm{disc}(e_1, \ldots, e_n) = \det(\mathrm{Tr}_{L/K}(e_ie_j))$. If $\{e_1, \ldots, e_n\}$ is an A-basis for B, then the discriminant $\mathfrak{d}_{B/A}$ is the ideal of A generated by $\mathrm{disc}(e_1, \ldots, e_n) \in A$.

It is standard that determinants of trace forms of A-bases are unique up to $A^\times$, so the ideal $\mathfrak{d}_{B/A}$ is well-defined.

Theorem 3.5 ([6], III.§5 Theorem 1, simplified)**.** *The discriminant $\mathfrak{d}_{B/A}$ is the unit ideal if and only if L/K is unramified.*

Proof. Let L/K have ramification index e and inertial degree f. We have $ef = n = [L : K]$. Suppose we have an A-basis e_i of B as above; then as A is a DVR we have $\mathfrak{d}_{B/A} = A$ if and only if $\mathrm{disc}(e_1, \ldots, e_n) \notin \mathfrak{m}_A$. Consider the κ_A-algebra $B/\mathfrak{m}_AB$ and denote this as R. As $\dim_{\kappa_A} R = \dim_{\kappa_B} R \dim_{\kappa_A} \kappa_B = ef = n$, and if we denote $\overline{e_i}$ the image of e_i after modding out by $\mathfrak{m}_A$, it follows that the $\overline{e_i}$ form a κ_A-basis of R as they span R and there are n of them. Since $\overline{\mathrm{Tr}_{L/K}(e_ie_j)} = \mathrm{Tr}_{R/\kappa_A}(\overline{e_ie_j})$ in κ_A (we have $\mathrm{Tr}(e_ie_j) \in A$) it turns out that $\mathrm{disc}(e_1, \ldots, e_n) \notin \mathfrak{m}_A$ if and only if $\mathrm{disc}(\overline{e_1}, \ldots, \overline{e_n}) \neq 0$ in κ_A, defined using the trace pairing Tr_{R/κ_A}. So we show that $\mathrm{disc}(\overline{e_1}, \ldots, \overline{e_n}) \neq 0$ if and only if L/K is unramified.

Suppose L/K is ramified; suppose we have $e > 1$. Then obviously $R = B/\mathfrak{m}_AB = B/\mathfrak{m}_B^e$ has nilpotence, say $x \in R$ is nilpotent. Then the map $y \mapsto \mathrm{Tr}(xy)$ is zero for all $y \in R$, as xy is also nilpotent, and multiplication maps of nilpotent elements have trace zero which can be seen from its characteristic polynomial. For such x, write $x = \sum_{i=1}^n k_i\overline{e_i}$ for $k_i \in \kappa_A$, then $\sum_{i=1}^n k_i \mathrm{Tr}_{R/\kappa_A}(\overline{e_ie_j}) = \mathrm{Tr}_{R/\kappa_A}(x\overline{e_j}) = 0$ for all $j = 1, \ldots, n$.

Writing $T_{ij} = \mathrm{Tr}_{R/\kappa}(\overline{e_i e_j})$, this means that $\sum_{i=1}^n k_i T_{ij} = 0$ for every j, i.e., the column vectors of (T_{ij}) admit a nontrivial κ_A-relation (as x itself is nonzero, the k_i cannot all be zero). This implies disc $= 0$. Now if $e = 1$ but κ_B/κ_A is not separable, then as R is just κ_B, it turns out that the trace pairing is degenerate as mentioned above. In particular, pick a nonzero x such that $y \mapsto \mathrm{Tr}_{\kappa_B/\kappa_A}(xy)$ is identically zero and repeat the same argument.

Conversely, suppose L/K is unramified, i.e., $e = 1$ and κ_B/κ_A is separable. This means that R is just κ_B. Then the trace form $\mathrm{Tr}_{\kappa_B/\kappa_A}$ is nondegenerate, and as the $\overline{e_i}$ form a basis of κ_B it follows that disc $\neq 0$. ☐

So, knowing the discriminant will give us information about the ramification. To actually calculate the discriminant, let us return back to our setup where A is a complete DVR, K is its fraction field, L/K is a finite separable extension, and B is the integral closure of A inside L which is finite over A. Furthermore assume that the residue field κ_A of A is perfect which ensures separability of the residue extension. In this case we will show that B has an A-basis of the form $1, b, \ldots, b^{n-1}$, which simplifies the discriminant calculation to the discriminant of the minimal polynomial of b.

Proposition 3.6 ([6], III.§6 Prop. 12)**.** *Let A, B, K, L be as in 2.5, together with the assumption that L/K is separable and B/A is finite of degree n. Furthermore assume that κ_A is perfect. Then B has an A-basis of the form $1, b, \ldots, b^{n-1}$.*

Proof. Let e be the ramification index and $f = [\kappa_B : \kappa_A]$. Then we have $ef = n$. As κ_B/κ_A is finite separable, by the Primitive Element Theorem we have some $\bar{b} \in \kappa_B$ such that $\kappa_B = \kappa_A(\bar{b})$. Take a $b \in B^\times$ that restricts to this $\bar{b}$. We claim that the elements $b^i \pi_B^j$ for $0 \le i < f$ and $0 \le j < e$ form an A-basis of B. Since there are n of them, and B is rank n, it suffices to show that they span B. As every element of B is uniquely written as $u\pi_B^n$ for $u \in B^\times$, where $\pi_A = \pi_B^e$, the set $\mathrm{Span}_A(b^i \pi_B^j)$ for $0 \le j < e$ reaches all possible exponents of π_B. Also, as $\bar{b}$ generates κ_B, the elements $1, \bar{b}, \ldots, \bar{b}^{f-1}$ span the f-dimensional κ_A-vector space κ_B. So indeed $\mathrm{Span}_A(b^i \pi_B^j) = B$. We furthermore show that there is some monic polynomial of degree f in $A[x]$ such that its value at b (or any other element of B congruent to it mod π_B) is a uniformizer of B.

Consider the minimal polynomial $m_{\bar{b}} \in \kappa_A[x]$ of $\bar{b} \in \kappa_b$. This has degree f, and we can lift this $m_{\bar{b}}$ to a monic polynomial $g \in A[x]$. Since $\overline{g(b)} = m_{\bar{b}}(\bar{b}) = 0$ in κ_B, we have $g(b) \in \mathfrak{m}_B$, i.e., $v_B(g(b)) \ge 1$. Now if $v_B(g(b)) = 1$ then $g(b)$ is a uniformizer of B and we have found such a polynomial. Suppose $v_B(g(b)) > 1$; by the algebraic Taylor's formula we have $g(b + \pi_B) \equiv g(b) + \pi_B g'(b) \mod \pi_B^2$. Note that $\overline{g'(x)} = m'_{\bar{b}}(x)$ in κ_B, and since $m_{\bar{b}}$ is a separable polynomial, we must have $m'_{\bar{b}}(\bar{b}) \neq 0$ in κ_B as otherwise $m_{\bar{b}}$ would have a double root at $\bar{b}$. This means that $g'(b) \notin \mathfrak{m}_B$, so $v_B(g'(b)) = 0$ and $v_B(\pi_B g'(b)) = 1$. But as we assumed $g(b)$ has valuation ≥ 2, it follows that $g(b + \pi_B)$ is of valuation 1 by the congruence above. Since $b + \pi_B$ is congruent to b mod π_B, we can replace our b chosen in the paragraph above by $b + \pi_B$, and take our g as our wanted polynomial. After doing this, we may replace the π_B^j in the $b^i \pi_B^j$ above with $g(b)^j$, and hence $b^i g(b)^j$ for $0 \le i < f$ and $0 \le j < e$ form an A-basis of B. Furthermore, g is monic of degree f so there exists a division algorithm, and in fact $1, b, \ldots, b^{n-1}$ form an A-basis of B. ☐

As $1, b, \ldots, b^{n-1}$ is an A-basis of B, the discriminant $\mathfrak{d}_{B/A} = (\mathrm{disc}(1, b, \ldots, b^{n-1}))$ is equal to the discriminant of the minimal polynomial of b over A. In fact, the ideal itself is way simpler than the integral case, as it is always of the form $\mathfrak{m}_A^n$ for some $n \ge 0$, and knowing the exponent would be sufficient. We provide some examples:

Example 3.7. Consider the quadratic extension $\mathbb{Q}_5(\sqrt{5})/\mathbb{Q}_5$. The number 5 is obviously not a 5-adic square; the valuation would have to be $1/2$. The underlying ring extension is $\mathbb{Z}_5[\sqrt{5}]/\mathbb{Z}_5$, and here $1, \sqrt{5}$ is a $\mathbb{Z}_5$-basis of the extension. So we may calculate the discriminant using the minimal polynomial of $\sqrt{5}$, which is $x^2 - 5$. Its discriminant is $20 \in \mathbb{Z}_5$, which has 5-adic valuation 1, i.e., it is equal to (5). In particular by 3.5, we see that the extension $\mathbb{Q}_5(\sqrt{5})/\mathbb{Q}_5$ is ramified. However, the case $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is different, as the integral closure of $\mathbb{Z}_2$ in this extension is not $\mathbb{Z}_2[\sqrt{5}]$. This is because the element $\frac{1+\sqrt{5}}{2}$ satisfies the integral equation $x^2 - x - 1 = 0$ over $\mathbb{Z}_2$, but it contains 2 as a denominator, which is not possible over $\mathbb{Z}_2[\sqrt{5}]$. So in fact the integral closure is $\mathbb{Z}_2[\frac{1+\sqrt{5}}{2}]$, and the integral basis is $1, \frac{1+\sqrt{5}}{2}$. The discriminant of its minimal polynomial $x^2 - x - 1$ is 5, which has valuation 0 in $\mathbb{Z}_2$. So the discriminant is the unit ideal, and the extension is unramified.

In particular, as finite extensions of p-adic numbers have finite residue field, it follows that we can always find a generator $b \in B$ of the integral closure for finite extensions of p-adic numbers. From the example above, one can see that the discriminant of the global extension $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is 5 as it is $1 \mod 4$ (or (5), depending on what you like) and simply taking the valuation of this global discriminant agrees with the local discriminants. This is not a coincidence; in fact, we have the following theorem:

Theorem 3.8 ([6], III.§4 Prop. 9, Prop. 10, Cor.)**.** *Let A be a Dedekind domain, K its field of fractions, L/K a finite separable extension, and B is the integral closure of A inside L. For a multiplicative subset S of A, we have $S^{-1}\mathfrak{d}_{B/A} = \mathfrak{d}_{S^{-1}B/S^{-1}A}$. Furthermore if we assume that A and B are both DVRs, we have $\widehat{\mathfrak{d}_{B/A}} = \mathfrak{d}_{\widehat{B}/\widehat{A}}$.*

From this, we obtain a description of the splitting of prime ideals in the global case; namely, if we have the global discriminant $\mathfrak{d}$, then its completion with respect to a prime is the unit ideal if and only if the local extension is unramified, so we can pick out the ramified primes. As we have seen in 3.7, the global discriminant is 5, so the local extension at $p = 5$ is ramified. So to put it all together, if we have an extension B/A of Dedekind domains, then the primes of A that ramify are precisely those that divide the global discriminant ideal. This is justified by our discussion on the extensions of complete DVRs, and 3.8.

References

[1] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley series in mathematics. Addison-Wesley Publishing Company, 1969.

[2] N. Bourbaki. *Topological Vector Spaces.* Number pt. 1 in Elements of mathematics. Springer-Verlag, 1987.

[3] K. Conrad. Finite-dimensional topological vector spaces. Notes. https://kconrad.math.uconn.edu/blurbs/topology/finite-dim-TVS.pdf.

[4] T. Husain. *Topology and Maps.* International Scholars Forum. Springer US, 1977.

[5] J. Neukirch and N. Schappacher. *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[6] J.P. Serre and M.J. Greenberg. *Local Fields.* Graduate Texts in Mathematics. Springer New York, 2013.

[7] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2025.

[8] A.V. Sutherland. 18.785 number theory i lecture 10. Lecture notes. URL:https://math.mit.edu/classes/18.785/2017fa/LectureNotes10.pdf.