Ramification in arithmetic and geometry

April 8, 2018

It may seem strange that the idea of ramification shows up while studying extensions of number fields and maps between Riemann surfaces. Is this a coincidence, overuse of terminology, or is there a connection between the two? It turns out that there *is* a connection; it can be explained by a shared algebraic structure. The goal of this note is to describe this structure, and to explain how it appears in number theory and geometry.

1 Discrete Valuation Rings

The common algebraic structure goes by the name of discrete valuation rings. Here is the definition.

Definition 1. A *discrete valuation ring* (DVR) is an integral domain R along with a surjective function $v\colon \operatorname{frac} R \to \mathbf{Z} \cup \{+\infty\}$, called the *valuation*, which satisfies the following properties.

1. $v(a) = +\infty$ if and only if $a = 0$.
2. $v(ab) = v(a) + v(b)$.
3. $v(a + b) \geq \min(v(a), v(b))$.
4. $a \in R$ if and only if $v(a) \geq 0$.

We will shortly see three examples of DVRs—one from arithmetic, one from algebra, and one from geometry.

The valuation v is often omitted from the notation. This is harmless, because v is often clear from context. In fact, it turns out that there can only be one possible valuation function on a DVR (see Proposition 9).

1.1 DVRs in arithmetic

Let p be a prime number. Let $\mathbf{Z}_p \subset \mathbf{Q}$ be the set of rational numbers that can be expressed as a/b where a and b are integers and p does not divide b. Note that $\mathbf{Z}_p$ is a ring, and it contains $\mathbf{Z}$ as a sub-ring. In particular, its fraction field is $\mathbf{Q}$. We will shortly see that that $R = \mathbf{Z}_p$ becomes a DVR with an appropriate valuation $v = v_p$. To define v_p, observe that every non-zero rational number r can be written as

$$r = p^n \frac{a}{b},$$

where $n, a, b \in \mathbf{Z}$ and p does not divide a or b. Then we set $v_p(r) = n$. We also set $v_p(0) = +\infty$, as required. We must verify that v_p is a well-defined function on $\mathbf{Q}$. That is, we must check that if there are two ways of representing r as above, then both lead to the same value of $v(r)$. This is easy to do. More interesting (but still straightforward) is the following.

Proposition 2. *The ring $\mathbf{Z}_p$ along with the valuation v_p is a DVR.*

Remark 3. Let K be a number field (a finite extension of $\mathbf{Q}$), and $O_K \subset K$ the ring of integers. Let $\mathfrak{p} \subset O_K$ be a prime ideal. We can define $O_{K,\mathfrak{p}} \subset K$ along with a valuation $v_\mathfrak{p}$, which is a DVR, generalizing the example above.

1.2 DVRs in algebra

Let a be a complex number. Let $\mathbf{C}[x]_a \subset \mathbf{C}(x)$ be the set of rational functions that can be expressed as $p(x)/q(x)$, where $p(x)$ and $q(x)$ are polynomials and $q(a) \neq 0$. Note that $\mathbf{C}[x]_a$ is a ring, and contains the polynomial ring $\mathbf{C}[x]$ as a sub-ring. In particular, its fraction field is $\mathbf{C}(x)$. Let $f \in \mathbf{C}(x)$ be non-zero. Observe that f can be written as

$$f = (x-a)^n \frac{p(x)}{q(x)},$$

where $n \in \mathbf{Z}$, and $p(x), q(x) \in \mathbf{C}[x]$ are such that $p(a) \neq 0$ and $q(a) \neq 0$. Set $v(f) = n$. Set $v(0) = +\infty$, as required. It is easy to verify that v is well-defined.

Proposition 4. *The ring $\mathbf{C}[x]_a$ along with the valuation v_a is a DVR.*

1.3 DVRs in geometry

For our last example, we need some preparation. Let X be a topological space and $x \in X$. Let $F(X, x)$ be the set of pairs (U, f), where $U \subset X$ is an open subset containing x and f is a function $f\colon U \to \mathbf{C}$. Define an equivalence relation on $F(X,x)$ by saying $(U_1, f_1) \sim (U_2, f_2)$ if there exists an open set V containing x and contained in $U_1 \cap U_2$ such that and $f_1|_V = f_2|_V$. An equivalence class of this relation is called a *germ of a function* on X at x. Denote by $F_{X,x}$ the set of germs of functions on X at x.

Said simply, a germ of a fuction on X at x is a function defined in *some* open set containing x, with the understanding that two functions are considered the same if they agree on some (possibly smaller) open set containing x. For example, the constant function 1 on $\mathbf{R}$ and the characteristic function χ of the interval $[-1, 1]$ represent the same germ at $x = 0$. Strictly speaking, a germ is represented by a pair (U, f), but the U is often omitted.

The set of germs of functions on X at x naturally forms a ring—addition and multiplication come from addition and multiplication of functions.

Instead of considering all functions, we may restrict ourselves to continuous functions or smooth functions (if X is a manifold).

Suppose $U \subset X$ is an open set containing x. It is easy to see that we have an isomorphism

$$F_{X,x} \cong F_{U,x} \tag{1}$$

given by restriction of functions.

Likewise, if $\phi\colon X \to Y$ is a homeomorphism and $y = \phi(x)$, then we have an isomorphism

$$F_{Y,y} \cong F_{X,x} \tag{2}$$

given by $f \mapsto f \circ \phi$.

Now let X be a Riemann surface. Let $O_{X,x}$ be the be set of germs of holomorphic functions on X at x. Note that if we take a chart centered at x, namely an open set $U \subset X$ containing X and a homeomorphism $\phi\colon U \to V$, where $V \subset \mathbf{C}$ is an open subset such that $\phi(x) = 0$, then by combining Equation 1 and Equation 2, we get an isomorphism

$$O_{X,x} \cong O_{\mathbf{C},0}.$$

In particular, $O_{X,x}$ does not depend on X or x. This is not surprising; it is simply a reflection of the fact that locally near x, a Riemann surface "looks just like" $\mathbf{C}$ does near 0. Note that the isomorphism $O_{X,x} \cong O_{\mathbf{C},0}$ depends on the choice of a chart at x.

The ring $O_{\mathbf{C},0}$ is easy to identify. Recall that $\mathbf{C}[\![z]\!]$ denotes the ring of formal power series in a variable z. Let $\mathbf{C}[\![z]\!]_{\text{conv}}$ be the subset of $\mathbf{C}[\![z]\!]$ consisting of power series with a positive radius of convergence (positive includes $+\infty$). For example,

$f(z) = 1 + z + z^2 + \cdots$ lies in $\mathbf{C}[\![z]\!]_{\text{conv}}$, but $0! + 1!z + 2!z^2 + \cdots$ does not. Observe that $\mathbf{C}[\![z]\!]_{\text{conv}} \subset \mathbf{C}[\![z]\!]$ is a sub-ring.

Proposition 5. *The ring $O_{\mathbf{C},0}$ is isomorphic to $\mathbf{C}[\![z]\!]_{\text{conv}}$.*

Let us go back to $O_{X,x}$ and show that $O_{X,x}$ becomes a DVR with an appropriate valuation v_x. Let η be a non-zero germ of a holomorphic function on X at x represented by (U, f). Let n be the order of vanishing of f at x. Set

$$v_x(\eta) = n.$$

As usual, set $v_x(0) = +\infty$.

Proposition 6. *The ring $O_{X,x}$ along with the valuation v_x is a DVR.*

Let us understand the valuation explicitly on $O_{\mathbf{C},0} \cong \mathbf{C}[\![z]\!]_{\text{conv}}$. Let g be a power series

$$g(z) = \sum_{n \geq 0} a_n z^n.$$

Then $v(g)$ is the minimum n such that $a_n \neq 0$. Using the isomorphism $O_{X,x} \cong \mathbf{C}[\![z]\!]_{\text{conv}}$ given by a chart, we get an explicit description of v_x on $O_{X,x}$. If the image of $f \in O_{X,x}$ is the power series

$$g(z) = \sum_{n \geq 0} a_n z^n,$$

then $v(f)$ is the minimum n such that $a_n \neq 0$.

2 Algebraic properties of DVRs

Let R be a DVR with valuation v. Let $m \subset R$ be the set of elements that have positive valuation (including $+\infty$).

Proposition 7. *The set m is a maximal ideal of R. Every element in $R \setminus m$ is invertible. Consequently, m is the unique maximal ideal of R.*

A ring with a unique maximal ideal is called a *local* ring. Proposition 7 says that a DVR is a local ring.

Proposition 8. *Let $t \in R$ be an element with valuation 1. Then t generates m as an ideal. More generally, if $I \subset R$ is any ideal, and $t \in I$ is an element with minimum valuation, then t generates I as an ideal. Finally, if $I \subset R$ is a non-zero ideal, then $I = m^n$ for some $n \geq 0$.*

In particular, Proposition 8 says that R is a Principal Ideal Domain (PID). In fact, it says that the only ideals of R are $t^n R$ where $t \in R$ is an element of valuation 1.

An element in R with valuation 1 is called a *uniformizer* or *local parameter*. For example, p is a uniformizer in $\mathbf{Z}_p$, and z is a uniformizer in $O_{\mathbf{C},0}$.

Proposition 9. *Let $t \in R$ be a uniformizer. Every element $x \in R$ is of the form*

$$x = ut^n,$$

where $u \in R$ is a unit. Consequently, the valuation function v on $\operatorname{frac} R$ is unique.

3 Ramification

Let R and S be DVRs with valuations v_R and v_S. Let $\phi\colon R \to S$ be a ring homomorphism. Note that ϕ induces a map of fields $\operatorname{frac} R \to \operatorname{frac} S$, which we also denote by ϕ.

We can compare the two functions v_R and $v_S \circ \phi$ defined on R. Observe that $v_S \circ \phi\colon \operatorname{frac} R \to \mathbf{Z} \cup \{\infty\}$ is a function satisfying all the properties of a valuation, except possibly surjectivity. The following proposition says that such a function must be a scaled version of the valuation function.

Proposition 10. *Let R be a DVR with valuation v. If $v' : R \to \mathbf{Z}_{\geq 0}$ is any function satisfying*

$$v'(ab) = v'(a) + v'(b),$$

then there exists a positive integer d such that

$$v'(a) = d \cdot v(a)$$

for all $a \in R$.

As a result, we conclude that there exists a d such that

$$v_S \circ \phi(a) = d \cdot v(a)$$

for all $a \in R$. We say that this integer d is the *multiplicity* of $\phi\colon R \to S$.

Example 11. Let $\phi\colon X \to Y$ be a non-constant holomorphic map between Riemann surfaces. Let $x \in X$ and set $y = \phi(x)$. The map ϕ induces a ring homomorphism

$$\phi^{\#} : O_{Y,y} \to O_{X,x}$$

defined by $\phi^{\#}(f) = f \circ \phi$. Then the multiplicity of $\phi^{\#}$ is the local multiplicity of ϕ at x.

Example 12. Let K be a number field, $O_K \subset K$ its ring of integers, and $\mathfrak{p} \subset O_K$ a prime ideal. Let $\mathbf{Z} \cap \mathfrak{p} = p\mathbf{Z}$. The inclusion $\mathbf{Z} \to O_K$ induces a map

$$\phi\colon \mathbf{Z}_p \to O_{K,\mathfrak{p}}.$$

Then the multiplicity of ϕ is the power of $\mathfrak{p}$ in the factorization of p into prime ideals of O_K.