# LECTURE 17, THURSDAY APRIL 15, 2004

FRANZ LEMMERMEYER

## 1. Discrete Valuation Rings

We say that a ring $R$ is a **discrete valuation ring** if $R$ is a Noetherian local ring whose maximal ideal is principal. The reason for this name is that we can define a function $v : R \setminus \{0\} \longrightarrow \mathbb{N}$ by putting $v(r) = n$ for $r = ut^n$. This function has the following properties:

(1) $v(r) \ge 0$ for all $r \in R$ (even for $r = 0$ if you put $v(0) = \infty$);
(2) $v(r) \ge 1$ if and only if $r \in \mathfrak{m}$; $v(r) = 0$ if and only if $r$ is a unit;
(3) $v(rs) = v(r) + v(s)$ for all $r, s \in R$;
(4) $v(r + s) \ge \min\{v(r), v(s)\}$.

The proofs are almost trivial; let us look at the last one and write $r = ut^n$, $s = vt^m$. If $n < m$, then $v(r+s) = n = \min\{v(r), v(s)\}$. If $n = m$, then $v(r+s) \ge n$. That's it.

More generally, a valuation of $R$ is a map $v : R \longrightarrow \overline{\mathbb{R}}$ (where $\overline{\mathbb{R}}$ is the set of nonnegative reals with $\infty$ included) having the properties $v(rs) = v(r) + v(s)$ and $v(r+s) \ge \min\{v(r), v(s)\}$. The valuation is said to be discrete if the value set $v(R)$ is discrete in $\overline{\mathbb{R}}$, for example if $v(R) = \mathbb{N}$ as in the example above.

In less fancy terms, a discrete valuation ring is a ring with a unique prime $p$, and the valuation tells us how often an element is divisible by $p$.

Note that valuations may exist in rings other than discrete valuation rings; for example, the valuation attached to the discrete valuation ring $\mathbb{Z}_{(p)}$ is also a valuation on $\mathbb{Z}$. This means that for every prime $p$ there is a $p$-adic valuation in $\mathbb{Z}$.

**Lemma 1.1.** *Let $P = (a, b)$ be a point on $\mathcal{C}_f : f(X, Y) = 0$. Then $\mathfrak{m}_P(\mathcal{C}_f) = (x - a, y - b)$, where $x = X + (f)$ and $y = Y + (f)$.*

*Proof.* Since $x$ and $y$ are defined everywhere, they are contained in $\mathcal{O}_P(\mathcal{C}_f)$, and since $x - a$ and $y - b$ vanish at $P$, they are contained in $\mathfrak{m}_P(\mathcal{C}_f)$.

Conversely, let $g = \frac{r}{s}$ be defined at $P$; then $g \in \mathfrak{m}_P$ means that $r(a, b) = 0$. Thus the Taylor expansion of $r \in K[X, Y]$ around $(a, b)$ does not have a constant term, hence can be written in the form $r(X, Y) = (X - a)c + (Y - b)d$ for polynomials $c, d$ (this is because all the terms of higher degree are divisible by $X - a$ or $Y - b$. But then $g = \frac{r}{s} = (x - a)\frac{c}{s} + (y - a)\frac{d}{s}$, and the quotients $\frac{c}{s}, \frac{d}{s}$ are elements of $\mathcal{O}_P$. Thus $g \in (x - a, y - b)$. □

**Theorem 1.2.** *Let $\mathcal{C}_f : f(X, Y) = 0$ be an irreducible plane curve defined over some algebraically closed field $K$, and let $P \in \mathcal{C}_f(K)$, and assume that $P$ is simple (i.e., nonsingular). Then $\mathcal{O}_P(\mathcal{C}_f)$ is a discrete valuation ring. If $L : aX + bY + c = 0$ is a line through $P$, the image $\ell$ of $L$ in $\mathcal{O}_P(\mathcal{C}_f)$ is a uniformizer if and only if $L$ is not a tangent.*

*Proof.* Changing coordinates we may assume that $P = (0, 0)$ with tangent $Y = 0$, and that $L : X = 0$. We have to show that the maximal ideal $\mathfrak{m}_P(\mathcal{C}_f)$ is generated by $x = X + (f)$. From Lemma 1.1 we know that $\mathfrak{m}_P = (x, y)$. Since $P$ is simple with tangent $L$, the Taylor expansion of $f$ around $P$ has the form $f(X, Y) = Y+$ terms of higher order; the terms of higher order are divisible by $Y$ or by $X^2$, hence we can write $f(X, Y) = Yg - X^2h$ for polynomials $g, h$ with $g(X, Y) = 1+$ terms of higher order and $h \in K[X]$. Reducing modulo $f$ we find $yg = x^2h$ in $K(\mathcal{C}_f)$, hence $y = x^2h/g \in (x)$ because $g(P) = g(0, 0) = 1 \neq 0$. Thus $\mathfrak{m}_P = (x, y) = (x)$. □

For simple points $P$ we therefore have a valuation $\mathrm{ord}_P$ on the discrete valuation ring $\mathcal{O}_P(\mathcal{C}_f)$.