LECTURE 11, MONDAY 15.03.04

FRANZ LEMMERMEYER

Manin's Proof

Proof of Lemma 1. The claim is trivial for $n = 0$. If $P_{n-1} = \mathcal{O}$, then it holds for n and $n+1$. Now assume that the claim is true for some $n \ge 0$ with $P_{n-1} \ne \mathcal{O}$, and we show by induction that it holds for $n+1$. Assume that $P_{n+1} \ne \mathcal{O}$; we assume that $x_{n+1} = 0$ or $\deg f_{n+1} \le \deg g_{n+1}$ and derive a contradiction.

In both cases ($x_{n+1} = 0$ or $\deg f_{n+1} \le \deg g_{n+1}$) we see that $x_{n+1}|_\infty$ is finite, hence $t^{-1}x_{n+1}|_\infty = 0$. Now

$$y_{n+1}^2 = \frac{x_{n+1}^3 + ax_{n+1} + b}{t^3 + at + b}$$

implies that $y_{n+1}|_\infty = 0$. Since $(x_{n+1}, -y_{n+1}) + (x_n, y_n) + (t, 1) = \mathcal{O}$, the three points $(x_{n+1}, -y_{n+1})$, (x_n, y_n) and $(t, 1)$ are collinear. Comparing slopes shows that

$$y_{n+1} = \frac{1 - y_n}{t - x_n}(t - x_{n+1}) - 1,$$

hence

$$0 = y_{n+1}|_\infty = \Big\{\frac{1 - y_n}{1 - t^{-1}x_n}\,(1 - t^{-1}x_{n+1}) - 1\Big\}\Big|_\infty.$$

From $t^{-1}x_{n+1}|_\infty = 0$ we deduce that

$$\frac{1 - y_n}{1 - t^{-1}x_n}\Big|_\infty = 1.$$

But according to the addition formulas we have

$$x_{n+1} = \Big(\frac{1 - y_n}{t - x_n}\Big)^2(t^3 + at + b) - t - x_n,$$

and hence we find

$$\frac{x_{n+1}}{t} = \Big(\frac{1 - y_n}{1 - t^{-1}x_n}\Big)^2(1 + at^{-2} + bt^{-3}) - 1 - \frac{x_n}{t}.$$

The induction hypothesis then implies

$$0 = \frac{x_{n+1}}{t}\,\Big|_\infty \;=\; \Big\{\Big(\frac{1 - y_n}{1 - t^{-1}x_n}\Big)^2(1 + at^{-2} + bt^{-3}) - 1 - \frac{x_n}{t}\Big\}\Big|_\infty = -\frac{x_n}{t}\,\Big|_\infty \ne 0,$$

and this is the desired contradiction. The proof for $n \le 0$ is done similarly.

Proof of the Basic Relation. It remains to prove

$$d_{n-1} + d_{n+1} = 2d_n + 2. \tag{1}$$

This is the heart of the proof. Again (1) is trivially true of one of P_{n-1}, P_n or $P_{n+1} = \mathcal{O}$: if, for example, $P_n = \mathcal{O}$, then $x_{n-1} = x_{n+1} = t$ as well as $d_n = 0$ and $d_{n-1} = d_{n+1} = 1$. If $P_{n-1} = \mathcal{O}$, then $(x_n, y_n) = (t, 1)$, and the additions formula gives

$$x_{n+1} = \frac{t^4 - 2at^2 - 8bt + a^2}{4(t^3 + at + b)}.$$

Thus $d_{n-1} = 0$, $d_n = 1$, and $d_{n+1} = 4$ (because $(f_{n+1}, g_{n+1}) = 1$)

Thus we may assume that the points P_{n-1}, P_n and P_{n+1} are all different from $\mathcal{O}$. The addition formula then gives $P_{n-1} = P_n + (t, -1)$, hence

$$\begin{aligned} x_{n-1} &= \frac{-(tg_n + f_n)(tg_n - f_n)^2 + (1 + y_n)^2(t^3 + at + b)g_n^3}{g_n(tg_n - f_n)^2} \\ &= \frac{(tg_n + f_n)(tf_n + ag_n) + 2bg_n^2 + 2y_n(t^3 + at + b)g_n^2}{(tg_n - f_n)^2} \\ &= \frac{R}{(tg_n - f_n)^2}, \end{aligned} \tag{2}$$

where we have used $\lambda y_n^2 = x_n^3 + ax_n + b$. Similarly we get

$$\begin{aligned} x_{n+1} &= \frac{-(tg_n + f_n)(tg_n - f_n)^2 + (1 - y_n)^2(t^3 + at + b)g_n^3}{g_n(tg_n - f_n)^2} \\ &= \frac{(tg_n + f_n)(tf_n + ag_n) + 2bg_n^2 - 2y_n(t^3 + at + b)g_n^2}{(tg_n - f_n)^2} \\ &= \frac{S}{(tg_n - f_n)^2}. \end{aligned} \tag{3}$$

Here $R, S \in \mathbb{F}_q[t]$ since the denominators of y_n cancel: from $\lambda y^2 = x^3 + ax + b$ we see that $\lambda y_n^2 g_n^3$ is integral, hence so is $\lambda y_n g_n^2$. Multiplying the expressions for x_{n-1} and x_{n+1} we get

$$\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(tg_n - f_n)^4} = \frac{(tf_n - ag_n)^2 - 4bg_n(tg_n + f_n)}{(tg_n - f_n)^2}. \tag{4}$$

If we can show that

$$g_{n-1}g_{n+1} = c \cdot (tg_n - f_n)^2 \tag{5}$$

for some $c \in \mathbb{F}_q$, then we find

$$f_{n-1}f_{n+1} = c[(tf_n - ag_n)^2 - 4bg_n(tg_n + f_n)]$$

and, using Lemma 1, that

$$d_{n-1} + d_{n+1} = \deg(f_{n-1}f_{n+1}) = \deg(t^2 f_n^2) = 2d_n + 2,$$

which is the claimed relation.

Now we know from (4) that $(tg_n - f_n)^2 \mid RS$. Writing $(tg_n - f_n)^2 = R_1 S_1$ with $R_1 \mid R$ and $S_1 \mid S$, we see

$$x_{n-1} = \frac{R}{(tg_n - f_n)^2} = \frac{R/R_1}{S_1}.$$

Next $f_{n-1}/g_{n-1} = x_{n-1}$, hence $g_{n-1} \mid S_1$. Similarly we can show $g_{n+1} \mid R_1$, , i.e. $g_{n-1}g_{n+1} \mid (tg_n - f_n)^2$. It is therefore sufficient to show that

$$(tg_n - f_n)^2 \mid g_{n-1}g_{n+1}. \tag{6}$$

Assume this is false. Then there is some irreducible $f \in \mathbb{F}_q[t]$ with $2v_f(tg_n - f_n) > v_f(g_{n-1}g_{n+1})$. Then (4) implies that $f \mid T$ for $T = (tf_n - ag_n)^2 - 4bg_n(tg_n + f_n)$. If we can show that f divides R and S, then f divides the polynomials $(1 - y_n)(t^3 + at + b)g_n^2$ and $(1 + y_n)(t^3 + at + b)g_n^2$. But since $f \nmid g_n$ (if $f \mid g_n$, then f would also divide f_n and g_n, but they are coprime) and since f is irreducible, we must have $f \mid (t^3 + at + b)$. Dividing T by $tg_n - f$, we get

$$T = -(tg_n - f_n)[tf_n^2 + (t^3 - 2at - 4b)g_n] + (t^4 - 2at^2 - 8bt + a^2)g_n^2.$$

Thus $f \mid (t^4 - 2at^2 - 8bt + a^2)$, and together with $f \mid (t^3 + at + b)$ and

$$(3t^3 - 5at - 27b)(t^3 + at + b) - (3t^2 + a)(t^4 - 2at^2 - 8bt + a^2) = \Delta,$$

where $\Delta = -4a^3 - 27b^2$, this implies that f divides the constant $\Delta \neq 0$: contradiction.

It remains to show that $f \mid R$ and $f \mid S$. From $f \mid T$ and $T \mid RS$ we see that R or S is divisible by f. Assume we had $f \mid R$ and $f \nmid S$. Then from $x_{n+1} = f_{n+1}/g_{n+1}$ and (3) it would follow that $v_f(g_{n+1}) = v_f(tg_n - f_n)^2 > 0$. Since f_{n+1} and g_{n+1} are coprime, this implies

$$v_f(f_{n+1}) = 0. \tag{7}$$

Using (4) we now see that $0 < v_f(T) = v_f(f_{n-1}) - v_f(g_{n-1})$, i.e., $v_f(f_{n-1}) > v_f(g_{n-1})$. Since f_{n-1} and g_{n-1} are also coprime, we find

$$v_f(g_{n-1}) = 0. \tag{8}$$

Now (7) and (8) show that

$$v_f(g_{n-1}g_{n+1}) = v_f(tg_n - f_n)^2,$$

and this is the contradiction that finishes the proof.