Places on algebraic curves

March 10, 2008

Introduction

Give L an algebraic extension of $k(x)$ where x is an indeterminate, we have defined a lattice $\mathsf{Val}(L,k)$ which is a point-free description of the Riemann surface X associated to L/k. (The topology is such that the open correspond to the cofinite sets. Furthermore there is an extra point which corresponds to the trivial valuation ring L.)

We present here a fundamental algorithm which of L enumerates *all* places P where a given non zero element f of L satisfies $v_P(f) > 0$ (that is, all places P where f is zero). From this algorithm follows for instance that the lattice $\mathsf{Val}(L,k)$ is *decidable*. It shows also how to represent any divisor of X as a formal sum of places. (Surprisingly it does not seem possible to associate a place to an arbitrary point of X.) We can also use this algorithm to define what are the poles of a given differential over X.

To simplify we suppose that k is algebraically closed. Using the technique of [2] we know how to make constructive sense of this assumption. In practice it means that when we have a polynomial we introduce new *symbols* with constraints that they have to be a root of this polynomial. These symbols are treated uniformely until some questions about them (for instance are they also root of another polynomial?) partition them in smaller groups.

In [5, 6], Edwards does not assume the field of constants to be algebraically closed but introduces instead extension when needed. It seems simpler to work from an algebraically closed field and to interpret the computations over it in a dynamic way. Since all computations are done in term of polynomials (without having to decide irreducibility but only computing gcd) it seems likely that the main results (for instance decidability of the lattice $\mathsf{Val}(L,k)$) hold without the hypothesis that k is algebraically closed.

We assume that L is determined by an equation $\chi(x,y) = y^n + p_1(x)y^{n-1} + \ldots + p_n(x) = 0$ where $\chi(X,Y) = Y^n + p_1(X)Y^{n-1} + \ldots + p_n(X)$ is a polynomial of $k[X,Y]$ irreducible in $k(X)[Y]$.

1 What is a place?

A *place* of L is given by two parameters α, β of L such that $L = k(\alpha,\beta)$ and a polynomial $f(X,Y)$ in $k[X,Y]$ such that f is irreducible in $k(X)[Y]$ and $f(\alpha,\beta) = 0$ and, if we decompose f in homogeneous component $f = f_0 + f_1 + \ldots$ we have $f_0 = 0$ and $f_1 \neq 0$.

For instance for L given by $x^3 + y^3 - xy = 0$ we have that $\alpha = x - 1/2, \beta = y - 1/2$ satisfies $4\alpha^3 + 6\alpha^2 + \alpha + 4\beta^3 + 6\beta^2 + \beta - 4\alpha\beta = 0$ and this determines a place. But x, y with $x^3 + y^3 - xy$ is not a place.

For L given by $y^2 = x^4 - 1$ we have that $\alpha = 1/x, \beta = -1 + y/x^2$ is a place with the polynomial $\alpha^4 + \beta^2 + 2\beta$.

Any place P determines a discrete valuation function $v_P : L^\times \to \mathbb{Z}$ and a local parameter t, that is a non zero element t of L such that $v_P(t) = 1$ (which is α or β). To the function v_P is associated a valuation ring V_P which is a point of X. We may write P instead of V_P. For computing v_P we know that α or β is a local parameter. For instance if α is a local parameter we can express β as an element of $k[[\alpha]]$ and we build in this way a map from $L = k(\alpha, \beta)$ in $k((\alpha))$[1].

If P is a place given by α, β, we can write formally the open $X - \{P\}$ as the open $U_P = V(1/\alpha, 1/\beta)$.

Theorem 1.1 *V_P is the set of elements z of L such that $1 = V(1/\alpha, 1/\beta, z)$. Also $v_P(z) > 0$ iff $V(1/z) \leqslant V(1/\alpha, 1/\beta)$.*

Proof. We show that $v_P(1/z) \geqslant 0$ iff $1 = V(1/\alpha, 1/\beta, 1/z)$. The proof of the second statement is similar.

If we have $1 = V(1/\alpha, 1/\beta, 1/z)$ then we have a relation of the form $p\alpha + q\beta + rz = 1$ with p, q, r in $k[\alpha, \beta, z]$. We have also $v_P(\alpha) > 0$ and $v_P(\beta) > 0$. Since $p\alpha + q\beta + rz = 1$ we cannot have $v_P(z) > 0$ and hence $v_P(z) \leqslant 0$.

Conversely we assume $v_P(z) \leqslant 0$ and we prove $1 = V(1/\alpha, 1/\beta, 1/z)$. We know that we have a relation $a\alpha + b\beta + g(\alpha, \beta) = 0$ where the multiplicity of g is > 1 with $a \neq 0$ or $b \neq 0$. Assume for instance that $b \neq 0$. Using this relation and $L = k(\alpha, \beta)$ one can write any non zero element of L, and in particular z on the form $\alpha^l \cdot (1 + f\alpha/1 + g\alpha)$ with f, g in $k[\alpha, \beta]$. We have then $v_P(z) = l \geqslant 0$. It follows that $z\alpha^{-l}(1 + g\alpha) = 1 + f\alpha$ and we have $1 = V(1/\alpha, 1/\beta, 1/z)$. □

It follows from this result that for any formal open U of $\mathsf{Val}(L, k)$ we have $U \leqslant U_P$ or $U_P \vee U = 1$.

Notice that membership $P \in V(f)$ is decidable since this is equivalent to $v_P(f) \geqslant 0$.

2 A fundamental algorithm

Given a non zero element f of L we are going to determine all places $P = P_1, \ldots, P_m$ such that $v_P(f) < 0$. Another statement is that $V(f) = X - \{P_1, \ldots, P_m\}$ in the lattice $\mathsf{Val}(L, k)$. Intuitively the places $P_1, \ldots, P_m$ are the *poles* of the function f. Here is yet another (formal) statement.

Theorem 2.1 *For any non zero element f of L there exists $P_1, \ldots, P_m$ places of L/k such that $V(f) = U_{P_1} \wedge \ldots \wedge U_{P_m}$.*

We can state a direct corollary.

Theorem 2.2 *The lattice $\mathsf{Val}(L, k)$ is* decidable.

Corollary 2.3 *In the field L it is decidable if an element f belongs to the integral closure $E(x)$ of $k[x]$.*

Proof. Indeed this is the case iff we have $v_P(x) < 0$ for all places P such that $v_P(f) < 0$ and we can compute all such places by Theorem 2.1. We then have $V(f) = U_{P_1} \wedge \ldots \wedge U_{P_m}$ and $V(x) \leqslant U_{P_1} \wedge \ldots \wedge U_{P_m}$ and hence $V(x) \leqslant V(f)$ in $\mathsf{Val}(L, k)$. By the characterisation of $\mathsf{Val}(L, k)$ this implies that f is integral over $k[x]$. □

[1] All this is finite and it might be interesting to have a finite construction which does not go via infinite formal series.

We proceed now to the proof of Theorem 2.1. The proof follows closely Abhyankar [1]. There seems to be some variations of the argument in [3, 4], which use Newton's polygon, but the algorithm itself and the proof of termination of the algorithm is much clearer in [1]. There is a similar argument in [6], which uses also Newton's polygon[2]. The argument of termination in Edwards if the same as in [1] (and he points out that the proof of termination in another standard reference, a book by Walker, is not constructive).

Since $P \in V(f)$ is decidable it is enough to find $P_1, \ldots, P_m$ places of L/k such that $U_{P_1} \wedge \ldots \wedge U_{P_m} \leqslant V(f)$. Since $1 = V(x) \vee V(1/x)$, it is enough to find $P_1, \ldots, P_m$ places of L/k such that $V(x) \wedge U_{P_1} \wedge \ldots \wedge U_{P_m} \leqslant V(f)$ and $Q_1, \ldots, Q_l$ places of L/k such that $V(1/x) \wedge U_{Q_1} \wedge \ldots \wedge U_{Q_l} \leqslant V(f)$. We show how to find $P_1, \ldots, P_m$ places of L/k such that $V(x) \wedge U_{P_1} \wedge \ldots \wedge U_{P_m} \leqslant V(f)$, the other problem being similar, changing x to $1/x$ and y to y/x^n such that y/x^n is integral over $k[1/x]$.

We write $f = p(x,y)/q(x,y)$. It is then enough to find all places P where x is finite (that is $v_P(x) \geqslant 0$) and where $q(x,y) = 0$ (that is $v_P(q) > 0$).

So we eliminate y between $q(x,y) = 0$ and $\chi(x,y) = 0$ finding a polynomial $\phi(x) = 0$ and for all a in k such that $\phi(a) = 0$ we compute the gcd $\psi_a(Y)$ of $q(a,Y)$ and $\chi(a,Y)$. For all root b of $\psi_a(Y)$ we must find all places P where $x = a$ and $y = b$.

2.1 Main Lemma

Lemma 2.4 *Given a, b in k such that $\chi(a,b) = 0$ find all places P where $x = a$ and $y = b$ (that is $v_P(x-a) > 0$ and $v_P(y-b) > 0$).*

Proof. This is achieved by a tree algorithm. At each node of the tree we have two parameters x_l, y_l such that $k(x_l, y_l) = L$. Furthermore we have $f^{(l)}(X,Y)$ such that $f^{(l)}(0,0) = 0$ and $f^{(l)}$ is irreducible in $k(X)[Y]$. At the root of the tree we have $x_0 = x - a$, $y_0 = y - b$ and $f^{(0)}(X,Y) = \chi(a+X, b+Y)$. We stop as soon as $0,0$ is a simple zero of $f^{(l)}(X,Y)$.

At one node x, y, g we write g as a sum of homogeneous polynomials $g = g_d + g_{d+1} + \ldots$ with $g_d \neq 0$. The number d is the *multiplicity* of the node. We know $d > 0$ and we stop if $d = 1$. So we can assume $d > 1$.

We try first to find, among all places P such that $v_P(x) > 0, v_P(y) > 0$ all places P such that $x/y = 0$ (and then all places P such that $v_P(y/x) \geqslant 0$). So we do the quadratic change of coordinate $x = uy$ and compute

$$g(uy, y) = y^d(g_d(u,1) + yg_{d+1}(u,1) + \ldots)$$

and the new polynomial is $h(u,y) = g_d(u,1) + yg_{d+1}(u,1) + \ldots$ [3] We check if 0 is a root of the polynomial $h(U,0) = g_d(U,1)$. Notice that a necessary condition for the multiplicity of the new system u, y, h to not decrease is that $g_d(U,1) = U^d$ (up to a multiplicative constant) and then the new multiplicity is the same.

We try then to find among all places P where $x = y = 0$ all places P such that $v_P(y/x) \geqslant 0$. So we do the quadratic change of coordinate $y = xt$ and compute

$$g(x, xt) = x^d(g_d(1,t) + xg_{d+1}(1,t) + \ldots) = x^d g'(x,t)$$

and we look at all roots of $g'(0,T) = g_d(1,T)$. Let these roots be $a_1, \ldots, a_e$ with $e \leqslant d$. For each i we form the new system $x, t - a_i, g^{(i)} = g'(X, a_i + T)$. A necessary for the multiplicity

[2] Let us cite Lagrange: "mais comme la méthode ... dépend du *parallélogramme* de Newton, et par conséquent ne peut être regardée que comme une méthode mécanique, je crois que les Géomètres seront bien aises de voir comment on peut résoudre cette question par une méthode purement analytique."

[3] It can be checked that $h(U,Y)$ is irreducible in $k(U)[Y]$.

not to decrease is that $g_d(1,T) = T^d$ and that $e = 1$ and we have only one root a_1. In this case we have that $g_d^{(1)}(X,T)$ of the form $T^d + \ldots$

This ends the description of the algorithm. We see that either the multiplicity decreases or we have only *one* descendant. Furthermore if the multiplicity does not decrease we should have $g_d(X,Y) = X^d$ or $g_d(X,Y)$ is of the form $(Y - aX)^d$.

Thus they are two cases where the multiplicity does not decrease. In one case we have a sequence of transformations

$$x = yx_1, y = y_1,\ x_1 = y_1x_2, y_1 = y_2,\ x_2 = y_2x_3, y_2 = y_3,\ \ldots$$

and in other case we have a sequence of transformation of the form

$$x = x_1, y = x(y_1 + a_1),\ x_1 = x_2, y_1 = x_1(y_2 + a_2),\ x_2 = x_3, y_2 = x_2(y_3 + a_3),\ \ldots$$

We show that this has to stop in both cases. The argument is the same, so we look at the second case (this termination argument appears in [1] and in other form in [5, 6].). We use here that $g(X,Y)$ and $g'_Y(X,Y)$ are such that there exists $r(X,Y), s(X,Y), \delta(X)$ such that

$$r(X,Y)g(X,Y) + s(X,Y)g'_Y(X,Y) = \delta(X)$$

with d non zero. This follows from the fact that $g(X,Y)$ is irreducible in $k(X)[Y]$. We see also that X^{2m} divides $g(X, a_1X + a_2X^2 + \ldots + a_mX^m + X^mY)$ and X^m divides $g'_Y(X, a_1X + a_2X^2 + \ldots + a_mX^m + X^mY)$. If follows that X^m divides $\delta(X)$ and hence the number of steps is limited a priori by the mutiplicity of 0 as a root of $\delta(X)$.

In this way we compute *all* places P such that $v_P(x - a) > 0$ and $v_P(y - b) > 0$. □

2.2 Examples

2.2.1 Example 1

$y^2 = 1 - x^4$: we find all places P where $x = 0, y = 1$

We first do the translation $x = x_0, y = y_0 + 1$. We get the equation $2y_0 + y_0^2 = 1 - x_0^4$ and we stop. We have a place P with the local parameter x_0. We have $v_P(y - 1) = 2,\ v_P(x) = 1$.

2.2.2 Example 2

$x^3 + y^3 = xy$: we find all places P where $x = 0, y = 0$

We first change $x = yu$ and look for places where $u = 0$. We get the equation $u = y(u^3 + 1)$. We have a place P_1 such that $v_{P_1}(y) = 1,\ v_{P_1}(x) = 2$ and u, y are local parameters.

We try next $y = xt$. We get the equation $t = x(t^3 + 1)$. We have a place P_2 such that $v_{P_2}(x) = 1,\ v_{P_2}(y) = 2$ and x, t are local parameters.

2.2.3 Example 3

$y^3 = x^2(1 - x)$: we find all places P where $x = 0, y = 0$

We first change $x = yu$ and look for places where $u = 0$. We get the equation $y = u^2(1 - yu)$. We have a place P_1 with local parameter u and such that $v_{P_1}(y) = 2,\ v_{P_1}(x) = 3$.

We try next $y = xt$. We get the equation $xt^3 = 1 - x$ and there are no places such that $v_P(t) \geqslant 0, v_P(x) > 0, v_P(y) > 0$.

2.2.4 Example 4

$(x^2+y^2)^3 = 4x^2y^2$: we find all places P where $x=0, y=0$

(This example is given at the beginning of [3].) We first change $x = yu$ and look for places where $u = 0$. We get the equation $y^2(1+u^2)^3 = 4u^2$. We then do the change $y = u(2+z)$ and find $(4+4z+z^2)(1+3u^2+3u^4+1) = 4$. Hence we have a place P_1 determined by $u = 0, z = 0$ with a local parameter u. We have $v_{P_1}(y) = 1$ and $v_{P_1}(x) = 2$. We have another place P_2 with the change $y = u(-2+z)$.

By symmetry we find two other place P_3, P_4 such that $v_{P_i}(x) = 1$ and $v_{P_i}(y) = 2$.

Since this algorithm proceeds only by simple quadratic transformations, it seems more "primitive" than the algorithms in [3, 6, 4] that use Newton's algorithm. Furthermore it computes at the same time a local parameter.

3 Application: integral basis

We consider now the case where k is the algebraic closure of $\mathbb{Q}$.

We want to show that the integral closure $E(x)$ of $k[x]$ in L is a free module over $k[x]$. We follow the algorithm in [6]. We compute the determinant of the matrix $tr_x(y^{i-1}y^{j-1})$ which is a polynomial in x and find its square factors $q(x)^2$. We then look at elements $p_0 + \ldots + p_{n-1}y^{n-1}/q$ that are integrals with $deg(p_i) < deg(q)$. For this we compute all places P such that $v_P(x) \geqslant 0$ and $v_P(q) > 0$ and a local parameter at each such place. For the element $f = p_0 + \ldots + p_{n-1}y^{n-1}/q$ to be in $E(x)$ the condition is that $v_P(f) \geqslant 0$ for all such places. This condition is a linear system of equations in term of the coefficient of $p_0, \ldots, p_{n-1}$.

For instance for the equation $x^3 + y^3 = xy$, we find $q = x$ (cf. Example 1 of Essay 4.5 [6]). We have then to decide when $f = a + by + cy^2/x$ is integral over $k[x]$. We have computed the two places P_1, P_2 such that $v_P(x) > 0$. The place P_1 is given by $u = x/y, y$ and y is a local parameter with $x = uy = y^2(1+u^3)$. We have $v_{P_1}(f) \geqslant 0$ iff $a = b = 0$. For P_2 we have $t = y/x$ and x local parameters and $y = x^2(1+t^3)$. Thus $v_{P_2}(f) \geqslant 0$ iff $a = 0$. In conclusion, a basis of $E(x)$ over $k[x]$ is $1, y, y^2/x$.

Another example if the Klein curve $y^3 + x^3y + x = 0$ (cf. Example 2 of Essay 4.5 [6]). Here also $q = x$ and we have to decide when $f = a + by + cy^2/x$ is integral over $k[x]$. There is only one place P such that $v_P(x) > 0$ and it is given by x, y and y is a local parameter with $x = -y^3 - yx^3$. Thus $v_P(f) \geqslant 0$ iff $a = b = c = 0$ and a basis of $E(x)$ over $k[x]$ is $1, y, y^2$.

Conclusion

It should now be possible to reconstruct all the main results of [5] Chapter 3. We can define the order of a differential at a place P and define a differential ω to be holomorphic if we have $v_P(\omega) \geqslant 0$ at all places. This definition should be shown equivalent with the more global definition in term of traces. There should be no obstacles also to obtain Riemann-Roch's Theorem with its usual formulation.

References

[1] S.S. Abhyankar. *Algebraic geometry for scientists and engineers.* Mathematical surveys and monographs, 35, American Mathematical Society, 1990.

[2] M. Coste, H. Lombardi, and M.F. Roy. Dynamical methods in algebra: effective Nullstellensätze, *Annals of Pure and Applied Logic* **111**(3):203–256, 2001.

[3] D.Duval. Rational Puiseux expansions. *Composition Mathematica* **70** : 119-154, 1989.

[4] D. Kozen. Efficient resolution of singularities of plane curves. LNCS 880, p. 1-11, 1994.

[5] H.M. Edwards. *Divisor Theory.* Birkauser Boston, 1990.

[6] H.M. Edwards. *Essays in Constructive Mathematics.* Springer-Verlag, New York, 2005.