Global divisors on an algebraic curve

January 13, 2008

Introduction

The goal of this note is to give an elementary definition of the divisor class group of an algebraic curve. We also explicitate in some special case Serre's duality Theorem. (This summarises discussions with Henri Lombardi, Claude Quitté and Peter Schuster.)

1 Space of valuations

If L is a field and R a subring of L, we define the lattice $\mathsf{Val}(L, R)$ as the lattice generated by symbols $V_R(s)$ for s in L with the relations

1. $1 = V_R(r)$ if r is in R
2. $V_R(s) \wedge V_R(t) \leqslant V_R(s+t)$
3. $V_R(s) \wedge V_R(t) \leqslant V_R(st)$
4. $1 = V_R(s) \vee V_R(s^{-1})$ if $s \neq 0$

Contrary to the Zariski lattice, we cannot in general simplify an expression $V_R(s_1) \wedge \ldots \wedge V(s_n)$ to a single basic open $V_R(s)$. Two exceptions can be noticed. We always have $V_R(r_1^{-1}) \wedge V_R(r_2^{-1}) = V_R((r_1r_2)^{-1})$ if $r_1,\ r_2$ non zero elements in R. For any non zero s in L we have

$$V_R(s) \wedge V_R(s^{-1}) = V_R(s + s^{-1})$$

Another useful general relation is

$$V_R((s_1 + s_2)^{-1}) \leqslant V_R(s_1^{-1}) \vee V_R(s_2^{-1})$$

The following Nullstellensatz result is proved by algebraic elimination.

Theorem 1.1 *We have $1 = V_R(s/t_1) \vee \ldots \vee V_R(s/t_n)$ iff s is integral over the ideal generated by $t_1, \ldots, t_n$.*

That s is integral over the ideal I generated by $t_1, \ldots, t_n$ means that we can find a relation $s^m + a_1 s^{m-1} + \ldots + a_m = 0$ with a_1 in I, …, a_m in I^m.

2 Zariski lattice

If R is an arbitrary ring, we define, following Joyal [11] the lattice $\mathsf{Zar}(R)$ as the lattice generated by symbols $D(a)$ for a in R with the relations

1. $1 = D(1)$ and $0 = D(0)$
2. $D(ab) = D(a) \wedge D(b)$
3. $D(a + b) \leqslant D(a) \vee D(b)$

Any element of $\mathsf{Zar}(R)$ can be written on the form $0,\ 1$ or $D(a_1, \dots, a_n) = D(a_1) \vee \dots D(a_n)$. In general we cannot simplify an union. However we can notice the general identity $D(a, b) = D(a + b, ab)$, from which follows the fact that $D(a, b) = D(a + b)$ if $D(ab) = 0$.

Theorem 2.1 *We have $D(a) \leqslant D(b_1, \dots, b_m)$ iff a belongs to the radical of the ideal generated by $b_1, \dots, b_m$.*

If now R is an integral domain and L its field of fractions, we have two lattices associated to R. By using the universal property of $\mathsf{Val}(L, R)$ one can define the center map

$$\phi : \mathsf{Zar}(R) \to \mathsf{Val}(L, R), \qquad D(r) \longmapsto V_R(1/r)$$

One can show that the center map is always injective and has the going-down property, using Theorem 1.1 in an essential way.

Remark: Skolem found a way to prove the disjunction property for intuitionistic logic without using cut-elimination. (This is called "sconing".) Can one use similar techniques to prove injectivity of the center map without going via cut-elimination?

3 Prüfer domain

A domain R is Prüfer iff it is locally at each prime a valuation domain. This can be captured by a simple first-order (coherent) condition [4]

$$\forall a\ b.\ \ \exists u\ v\ w.\ \ au = bv \wedge b(1 - u) = aw$$

If we write $s = a/b$ and we have $au = bv$ and $b(1 - u) = aw$ then we can check that we have $V_R(s) = V_R(1/u) \vee V_R(1/w)$ in $\mathsf{Val}(L, R)$.

Proposition 3.1 *If R is a Prüfer domain, the center map is bijective. If $s = a/b$ is in L the inverse image of $V_R(s)$ is $D(u, w)$ such that we have $au = bv$ and $b(1 - u) = aw$.*

Since we know that the center map is injective, it is enough to show that it is surjective and this follows from the equality $V_R(s) = V_R(1/u) \vee V_R(1/w)$.

The fact that the center map is bijective can be proved *without* cut-elimination. For instance, notice that this inverse map is well-defined, for if we have also $au_1 = bv_1$ and $b(1 - u_1) = aw_1$ then we have $D(u, w) = D(u_1, w_1)$ in $\mathsf{Zar}(R)$. Indeed we have $u_1(1 - u) = wv_1$ and hence $D(u_1) \leqslant D(u, w)$ and $(1 - u_1)w = (1 - u)w_1$ and hence $D(w_1) \leqslant D(u, w)$.

Conversely, it can be shown that if R is integrally closed and the center map is bijective then R is a Prüfer domain.

It is clear from the definition that if S is any domain containing R and inside L then S is also a Prüfer domain.

The following proposition can be proved by reasoning locally at each prime (and a pointfree version of this argument is possible).

Proposition 3.2 *If R is a Prüfer domain, L its field of fractions and we consider $s, t_1, \dots, t_n$ in L then s is integral over the ideal generated by $t_1, \dots, t_n$ iff s belongs to this ideal.*

This means that, if $t_1, \dots, t_n$ are non zero, then s belongs to the ideal generated by $t_1, \dots, t_n$ iff we have $1 = V_R(s/t_1) \vee \dots V_R(s/t_n)$ in $\mathsf{Val}(L, R)$.

Here is a simple application.

Corollary 3.3 *Let I_1, I_2 be two finitely generated fractional ideals over R and s any non zero element of S. Then $I_1 = I_2$ iff $I_1R[s] = I_2R[s]$ and $I_1R[1/s] = I_2R[1/s]$.*

Proof. We show that x belongs to I if it belongs to $IR[s]$ and $IR[1/s]$. Let $t_1, \dots, t_n$ be generators of I. By Proposition 3.2 we have

$$1 = V_{R[s]}(x/t_1) \vee \dots \vee V_{R[s]}(x/t_n), \qquad 1 = V_{R[1/s]}(x/t_1) \vee \dots \vee V_{R[1/s]}(x/t_n)$$

and hence

$$V_R(s) \leqslant V_R(x/t_1) \vee \dots \vee V_R(x/t_n), \qquad V_R(1/s) \leqslant V_R(x/t_1) \vee \dots \vee V_R(x/t_n)$$

and hence, since $1 = V_R(s) \vee V_R(1/s)$ we get $V_R(x/t_1) \vee \dots \vee V_R(x/t_n)$ □

To any Prüfer domain R we can associate a *lattice group* $\mathsf{Div}(R)$. The elements of $\mathsf{Div}(R)$ are non zero finitely generated fractional ideals. The group operation is the product of ideals. The order is the reverse of the inclusion order. The neutral element is the unit ideal R. The meet operation is the sum of ideals. The fact that it is a lattice group is proved in [4]. A consequence of this is that finitely generated ideals form a lattice, which is furthermore distributive.

If s is non zero we have two lattice maps $\mathsf{Div}(R) \to \mathsf{Div}(R[s])$ and $\mathsf{Div}(R) \to \mathsf{Div}(R[1/s])$.

Corollary 3.3 is complemented by the following glueing property.

Corollary 3.4 *If I in $\mathsf{Div}(R[s])$ and J in $\mathsf{Div}(R[1/s])$ are such that $IR[s, 1/s] = JR[s, 1/s]$ then there exists K (unique) in $\mathsf{Div}(R)$ such that $KR[s] = I$ and $KR[1/s] = J$.*

The following result has a simple constructive proof. We recall that a primitive polynomial in $R[X]$ is a polynomial $a_0 + \dots + a_nX^n$ such that $1 = D(a_0, \dots, a_n)$.

Proposition 3.5 *If R is integrally closed R is a Prüfer domain iff any s in L is the root of a primitive polynomial in $R[X]$.*

Corollary 3.6 *If L is a field containing a Bezout domain S and R the integral closure of S in L then R is a Prüfer domain.*

4 Algebraic curves

An algebraic curve over $\mathbb{Q}$ is an algebraic extension L of the field of rational functions $\mathbb{Q}(x)$. For instance we can take $y^2 = 1 - x^4$ but also $z^2 + x^2 + z^2x^2 = 1$ or $y^3 + x^3 = xy$ or $y^3 + x^3y + x = 0$.

If p is an element of L we have an polynomial relation $f(p, x) = 0$. We can then decide from this relation if p is algebraic over $\mathbb{Q}$ (in which case p is called a *constant* of L) or x is algebraic over $\mathbb{Q}(p)$ (in which case p is called a *parameter* of L).

To this algebraic extension we associate the lattice $X = \mathsf{Val}(L, \mathbb{Q})$. We write $V(s)$ instead of $V_{\mathbb{Q}}(s)$.

We associate various sheaves over the space X.

The structure sheaf $\mathcal{O}$ is defined by taking $\mathcal{O}(v)$ to be the ring of elements s such that $v \leqslant V(s)$ in $\mathsf{Val}(L, \mathbb{Q})$. In particular $\mathcal{O}(V(p))$ is the integral closure of $\mathbb{Q}[p]$. If $u_1, \dots, u_n$ are elements of L we write $E(u_1, \dots, u_p)$ the integral closure of $\mathbb{Q}[u_1, \dots, u_n]$ so that $\mathcal{O}(V(u_1) \wedge \dots V(u_n))$ is $E(u_1, \dots, u_n)$.

Another sheaf is the sheaf of holomorphic differentials. If p is a parameter of L then $E(p)$ is a $\mathbb{Q}$ algebra and we define $\Omega(V(p))$ to be the $E(p)$ module $\Omega_{E(p),\mathbb{Q}}$.

In good cases this should be a projective module of rank 1. For instance, for $y^2 = 1 - x^4$ we get the module with generators $dx,\ dy$ and relation

$$ydy - 2x^3dx = 0$$

which is a projective module of rank 1 since we have the relation $yy + (-2x^3)x/2 = 1$.

In general if L is defined by the equation $\chi(x, y) = 0$ then we get the module with generators $dx,\ dy$ and the equation is $\chi'_x dx + \chi'_y dy = 0$. The condition is thus that we have $<\chi'_x, \chi'_y> = 1$ in $E(x)$.

If we assume that we have a trace operation $tr : L \to \mathbb{Q}(x)$ then an equivalent definition of $\Omega(V(x))$ is to take the ideal of elements f in L such that $tr(fa) \in \mathbb{Q}[x]$ for all a in $E(x)$. A *global* holomorphic differential is then given by an element f in L such that $tr(fa) \in \mathbb{Q}[x]$ for all a in $E(x)$ *and* $tr(-fx^{-2}b) \in \mathbb{Q}[1/x]$ for all b in $E(1/x)$. The coefficient x^{-2} comes from the equality $fdx = -fx^{-2}d(1/x)$.

Remark: We have to find the right hypotheses so that the sheaf of holomorphic differentials is indeed a global projective module of rank 1 and so that we can show that the two definitions coincide.

The second definition of $\Omega(V(x))$ is convenient for computation once we know a basis of $E(x)$ over $\mathbb{Q}[x]$. For instance, in the example $y^2 = 1 - x^4$, we have that $1, y$ is a basis of $E(x)$ over $\mathbb{Q}[x]$. It follows that fdx is in $\Omega(V(x))$ iff $tr(f)$ and $tr(fy)$ are in $\mathbb{Q}[x]$. Since we can write $f = \alpha + y\beta$ with α and β in $\mathbb{Q}(x)$, we get that α is in $\mathbb{Q}[x]$ and $y^2\beta$ is in $\mathbb{Q}[x]$. In this way we get that $\Omega(V(x))$ is the $E(x)$ module generated by 1 and $1/y$. Similarly, if we take $u = 1/x$ and $v = y/x^2$ we have $v^2 = u^4 - 1$ and $\Omega(V(u))$ is the $E(u)$ module generated by 1 and $1/v$.

Notice that since $yy + (-2x^3)x/2 = 1$ we have $dx/y = dy/(-2x^3) = ydx + x/2dy$ which shows that dx/y is holomorphic over the open $V(x)$.

Hence a global holomorphic differential is of the form $r_1dx/y = -r_1du/v$ for some rational r_1.

We can check Serre's duality in the examples. For L defined by the equation $y^2 = 1 - x^4$ the pairing map consists in taking an element of $H^1(X, \mathcal{O})$ which is an element g of $E(x + x^{-1})/E(x) \oplus E(x^{-1})$, thus of the form r_0yx^{-1} with an element fdx of $H^0(X, \Omega)$ hence of the form $r_1y^{-1}dx$. One can guess that the pairing map should be in this case $< r_0y/x, r_1/y >= r_0r_1$.

5 Divisor class group

A *global divisor* on X can be defined as a pair of elements I in $\mathsf{Div}(E(x))$ and J in $\mathsf{Div}(E(1/x))$ such that $IE(x + 1/x) = JE(x + 1/x)$.

The following seems to provide a good concrete description of global divisors. A local divisor is given by a finite sequence of non zero elements of L. If A, B are such sequences we introduce the notation $A = B : E(u_1, \dots, u_n)$ to mean that we have $AE(u_1, \dots, u_n) = BE(u_1, \dots, u_n)$. A *global divisor* consists in giving a collection A_v of finite sequences for each non trivial basic open v of X in such a way that $A_v = A_{v'} : \mathcal{O}(v \wedge v')$ for each v, v'. It is equivalent to give A_x and $A_{1/x}$ in such a way that $A_x = A_{1/x} : E(x, 1/x)$ for *one* parameter x.

Remark: Is this valid? This would mean that if we have a Prüfer domain R and two finite sequences A, B such that $AR[s, 1/s] = BR[s, 1/s]$ then we can find C such that $CR[s] = AR[s]$ and $CR[1/s] = BR[1/s]$. I will see if one can find this in [4].

References

[1] J. Avigad. Methodology and metaphysics in the development of Dedekind's theory of ideals. Preprint 2005.

[2] N. Bourbaki. *Eléments de Mathématique. Algèbre commutative. Chapitre 7.* Paris, Hermann, 1965.

[3] R. Dedekind and H. Weber Theorie des algebraischen Funktionen einer Veränderlichen. *J. de Crelle*, t. XCII (1882), p. 181-290.

[4] L. Ducos, H. Lombardi, C. Quitté and M. Salou. Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind. J. Algebra 281 (2004), no. 2, 604–650.

[5] H.M. Edwards. The genesis of ideal theory. *Arch. Hist. Ex. Sci.*, pages 321–378, 1980.

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

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

[8] L. Espanol. The spectrum lattice of Baer rings and polynomials. *Categorical algebra and its applications (Louvain-La-Neuve, 1987)*, pages 118–124, 1988.

[9] K.F. Gauss. *Disquisitiones Arithmeticae.* 1802.

[10] P. Jaffard. *Théorie de la dimension dans les anneaux de polynomes.* Mémor. Sci. Math., Fasc. 146 Gauthier-Villars, Paris 1960.

[11] A. Joyal. Le théorème de Chevalley-Tarski. *Cahiers de Topologie et Géométrie Différentielle* 16, 256–258 (1975).

[12] P. T. Johnstone. *Stone Spaces.* Cambridge studies in advanced mathematics 3, 1982.

[13] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. reine angew. Math.* 92, 1-123 (1882). Reprinted in *Leopold Kronecker's Werke*, II, 237–387.

[14] L. Kronecker. Ein Fundamentalsatz der Allgemeinen Arithmetic. *J. reine angew. Math.* 100, 490-510 (1887).

[15] E. Dobbs, R. Fedder, and M. Fontana. Abstract riemann surfaces of integral domains and spectral spaces. *Ann. Mat. Pura Appl. (4) 148*, pages 101–115, 1987.

[16] R. Mines, F. Richman and W. Ruitenburg. *A course in constructive algebra.* Springer-Verlag, 1988

[17] F. Richman. Van der Waerden's construction of a splitting field. Communications in Algebra, Volume 34 Issue 7 2006.

[Sco74] D. Scott. Completeness and axiomatizability. *Proceedings of the Tarski Symposium, (1974), p. 411-435.*

[18] J.P. Serre. Faisceaux Algébriques Cohérents. Annals of Mathematics, 1955.

[19] M. Stone. Topological representations of distributive lattices and Brouwerian logics. Cas. Mat. Fys. 67, (1937), 1-35.

[20] L. Thery. Proving the group law for elliptic curves formally. to appear in the proceeding of TPHOL, 2007.

[21] G. C. Wraith. Intuitionistic algebra: some recent developments in topos theory. Proceedings of the International Congress of Mathematicians (Helsinki, 1978), pp. 331–337, Acad. Sci. Fennica, Helsinki, 1980.