A remark about the theory of local rings

March 10, 2008

We prove that in the theory of local rings it is not possible to show that to be invertible is decidable. This is a simple example of the technique of using the "classifying topos" to show non derivability of a formula by checking that this formula is not valid in this model.

1 Theory of local rings

The theory of local rings extends the equational theory of rings by the axiom

$$\forall x.\ (\exists y.\ xy = 1) \vee (\exists y.\ (1-x)y = 1)$$

If we introduce the notation $inv(x)$ for $\exists y.\ xy = 1$ this can be written simply as $inv(x) \vee inv(1-x)$. Since we have $inv(1)$ a formula which seems a priori more general would be

$$inv(x+y) \rightarrow (inv(x) \vee inv(y))$$

Actually both formulations are equivalent. Indeed if we assume $inv(u) \vee inv(1-u)$ for all u and $inv(x+y)$, let v be an inverse of $x+y$. We have then $vx + vy = 1$ and hence $inv(vx)$ or $inv(vy)$. Since we clearly have

$$inv(rs) \leftrightarrow (inv(r) \wedge inv(s))$$

for all r, s we deduce $inv(x)$ or $inv(y)$ as desired.

Classically, a local ring is a ring with only one maximal ideal. It is possible to define this ideal without using negation by introducing $J(x)$ to be $\forall y.\ inv(1-xy)$. In general this defines the *Jacobson radical* of the ring. If the ring has only one maximal ideal, this should be the Jacobson radical. Notice that we have

$$\forall y.\ \ inv(xy) \vee inv(1-xy)$$

and hence

$$\forall y.\ \ inv(x) \vee inv(1-xy)$$

Classically, it is possible to deduce $inv(x) \vee J(x)$.

The main goal of this note is to show that this is *not* valid intuitionistically. Intuitively, if you give an algorithm to decide $inv(x)$ or $inv(1-x)$ (and to give the corresponding inverse in each case) then it is not possible, using this algorithm as an oracle, to decide $inv(x)$ or $J(x)$.

The fact that we have $inv(x)$ or $J(x)$ is used classically in the following proof that any finitely generated projective module M over a local ring A is free. We have a basis of the vector space M/JM over the field A/J. Hence by Nakayama's Lemma, this basis gives a generating set of the module M over A, which is clearly also free, and so is a basis of M over A.

2 Generic local rings

For proving the non derivability of $inv(x) \vee J(x)$ we show that this formula does not hold in the generic model. This means that this formula is not *forced* for the forcing relation defined in [Coquand 2005].

We recall a possible presentation of this forcing relation. It is of the form $R \Vdash \phi$ where R is a finitely presented ring. The inductive clauses are

$R \Vdash t = u$ if $t = u$ in R

$R \Vdash \phi_1 \wedge \phi_2$ if $R \Vdash \phi_1$ and $R \Vdash \phi_2$

$R \Vdash \phi_1 \vee \phi_2$ if $R \Vdash \phi_1$ or $R \Vdash \phi_2$

$R \Vdash \phi_1 \rightarrow \phi_2$ if for all finitely presented extension $R \rightarrow S$ we have $S \Vdash \phi_2$ whenever $S \Vdash \phi_1$

$R \Vdash \forall x.\psi$ if for all finitely presented extension $R \rightarrow S$ we have $S \Vdash \psi(s)$ for all s in S

$R \Vdash \exists x.\psi$ if there exists u in R such that $R \Vdash \psi(u)$

$R \Vdash \phi$ if $R[x^{-1}] \Vdash \phi$ and $R[(1-x)^{-1}] \Vdash \phi$

It can be shown that we have $R \Vdash t_1 = t_2$ iff $t_1 = t_2$ in R.

Similarly, it can be shown that we have $R \Vdash \forall x.\psi$ iff $S \Vdash \psi(s)$ for all finitely presented extension S of R and all s in R.

Also $R \Vdash \exists x.\psi$ iff there exists $u_1, \ldots, u_n$ in R and t_i in $R[u_i^{-1}]$ such that $<u_1, \ldots, u_n> = 1$ and $R[u_i^{-1}] \Vdash \phi(t_i)$.

Similarly $R \Vdash \psi_0 \vee \psi_1$ iff there exists u_0, u_1 in R such that $<u_0, u_1> = 1$ and $R[u_i^{-1}] \Vdash \psi_i$.

Lemma 2.1 *We have $R \Vdash inv(x)$ iff x is invertible in R*

Proof. We have $u_1, \ldots, u_n$ in R and t_i in $R[u_i^{-1}]$ such that $<u_1, \ldots, u_n> = 1$ and $R[u_i^{-1}] \Vdash t_i x = 1$. We have then s_i in R and k such that $s_i x = u_i^k$. There exists α_i in R such that $1 = \Sigma u_i^k \alpha_i$ and then $x(\Sigma \alpha_i t_i) = 1$. □

Lemma 2.2 *We have $R \Vdash J(x)$ iff x is nilpotent in R*

Proof. If x is nilpotent we have n such that $x^n = 0$. Then for all y we have $\Sigma_{i<n}(xy)^i$ which is an inverse of $1 - xy$. So we have $S \Vdash inv(1 - xy)$ for all finitely presented extension $R \rightarrow S$ and all y in S.

Conversely assume $R \Vdash J(x)$. We consider the finite extension $R \rightarrow R[x^{-1}]$. Since we have $R \Vdash \forall y.inv(1 - xy)$ we should have $R[x^{-1}] \Vdash inv(1 - xy)(x^{-1}/x)$ and so $R[x^{-1}] \Vdash inv(0)$ which implies $R[x^{-1}] \Vdash 1 = 0$ by Lemma 2.1. Hence we have $1 = 0$ in $R[x^{-1}]$ and so x is nilpotent in R. □

Proposition 2.3 *If R is an integral domain and x non zero in R we have $R \Vdash inv(x) \vee J(x)$ iff x is invertible in R*

Proof. Assume $R \Vdash inv(x) \vee J(x)$. By Lemmas 2.1 and 2.2 we then have $1 = u_0 + u_1$ with x invertible in $R[u_0^{-1}]$ and x nilpotent in $R[u_1^{-1}]$. Since x is non zero, this implies $u_1 = 0$ and hence x is invertible in R. □

Corollary 2.4 *We do not have $\Vdash \forall x.\ inv(x) \vee J(x)$.*

Proof. We take $R = \mathbb{Z}$ and $x = 2$. Since x is non zero but not invertible in R we cannot have $\mathbb{Z} \Vdash inv(x) \vee J(x)$ by Proposition 2.3. □

3 Topological model

The last result suggests a simpler counter-model in a sheaf model over $X = \mathsf{Zar}(\mathbb{Z})$. For an open $U = D(m_1, \ldots, m_k)$ we define

$$\mathcal{O}(U) = \mathbb{Z}[1/m_1] \cap \ldots \cap \mathbb{Z}[1/m_k].$$

Then $\mathcal{O}$ is a sheaf of rings over X. This is a local ring.

We have $D(m) \Vdash J(2)$ only if $m = 0$. Indeed this implies $D(m2) \Vdash inv(0)$ and hence $m2 = m = 0$. So the interpretation of $J(2)$ is the empty open.

On the other have the interpretation of $inv(2)$ is the open $D(2)$. Since $X \neq D(2)$ we don't have $X \Vdash inv(2) \vee J(2)$.

References

[Coquand 2005] Th. Coquand. A Completness Proof for Geometrical Logic to appear, 2005.

[Coste *et al.*] 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.

[Mulvey] C. Mulvey. Intuitionistic algebra and representations of rings. In *Recent advances in the representation theory of rings and C^*-algebras by continuous sections*, pp. 3–57. Mem. Amer. Math. Soc., No. 148, Amer. Math. Soc., Providence, R. I., 1974.

[Reyes] G. Reyes. Théorie des modèles et faisceaux. *Adv. in Math.* 30 (1978), no. 2, 156–170.

[Warith] G. 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.