Exercises on the course on Constructive Logic

August 10, 2008

Exercises on intuitionistic logic

1. Prove that the schema $\neg\neg A \to A$ is equivalent to the law of excluded middle $A \vee \neg A$

2. (To get a feeling about the difference between constructive and classical reasoning.) Consider the sequence z_n in $[0,1]$ defined by $z_0 = 1$ and $z_{n+1} = z_n - z_n^2/2$. Prove classically that z_n converges to 0 as follows. First show that $0 \leqslant z_{n+1} \leqslant z_n$ and hence that z_n converges. Let l be the limit. Show that $l^2 = 0$ and hence $l = 0$. Where have we used the law of excluded-middle in this reasoning? This result implies that given $\epsilon > 0$ we can find N such that $z_N \leqslant \epsilon$. Try to see if we can extract such a N from this reasoning, and then find a constructive justification of the existence of such a N.

3. (Constructive version of classical results.) Show classically that if X is a compact metric space and $f : X \to X$ is such that $d(f(x), f(y)) < d(x, y)$ if $x \neq y$ then f has a unique fixed-point. For this, consider a point where the function $x \longmapsto d(x, f(x))$ is minimum. The goal of this exercice is to present a constructive reading of this result. The condition

$$x \neq y \to d(f(x), f(y)) < d(x, y)$$

can be written

$$(\exists n. d(x, y) \leqslant 1/2^n) \to (\exists m. d(f(x), f(y)) \leqslant (1 - 1/2^m) d(x, y))$$

A natural constructive reading is

$$\forall n \exists m.\ \ d(x, y) \leqslant 1/2^n \to d(f(x), f(y)) \leqslant (1 - 1/2^m) d(x, y)) \tag{1}$$

Show from (1) only that for any $\epsilon > 0$ and any a in X there exists N such that

$$d(f^{N+1}(a), f^N(a)) < \epsilon$$

Using (1), show also that we have

$$\forall \epsilon > 0. \exists \eta > 0.\ \ d(x, f(x)) < \eta \wedge d(y, f(y)) < \eta \to d(x, y) < \epsilon \tag{2}$$

Explain why (2) can be seen as a constructive reading of the implication

$$x = f(x) \wedge y = f(y) \to x = y$$

Using this, show constructively that if X is a metric space which satisfies (1) and is *complete* (no need of compactness) then f has a unique fixed-point, and furthermore, that for any point a in X the sequence $f^n(a)$ is a Cauchy sequence which converges to this fixed-point.

This example is extracted from the work of Ulrich Kohlenbach, who had developped remarkable constructive reading of multiple results in analysis (especially fixed-point theory) using techniques from logic.

4. Define in the theory of rings $J(x)$ as $\forall y.inv(1-xy)$, where $inv(x)$ means $\exists y.1 = xy$. Classically $J(x)$ means that x belongs to all maximal ideals. Prove this using Zorn's Lemma. It follows in particular that $J(x)$ defines an ideal and hence $J(x) \wedge J(y) \rightarrow J(x+y)$ is a semantical consequence of the theory of rings. Check the validity of the completeness theorem of the first-order theory of rings by giving a direct first-order proof of this implication.

5. The notion of principal ideal domain is subtle constructively: the classical notion involves a quantification over all ideals. Constructively, one tries to work instead with a first-order approximation, which is the notion of *Bezout domain*: any *finitely generated* ideal is principal. Check that this notion is first-order and is even coherent. Show that if K is a field then $K[X]$ is a Bezout domain. Show that a finitely generated of a submodule of R^n is free if R is a Bezout domain.

6. The notion of *Unique Factorization Domain* (any element is in a unique way a product of irreducible elements) is not a first-order notion. Constructively, one replaces this notion by the notion of *gcd domain*: for any a, b there exists g which divides a and b and such that if c divides a and b then c divides g. Check that this is a first-order notion. Show that such an element g is defined uniquely up to a unit. Such an element g is called a *gcd* of a and b. Show that any Bezout domain is a gcd domain.

   If R is a gcd domain we define the *content* of a polynomial P in $R[X]$ to be the gcd of all its coefficient, and we say that a polynomial is *primitive* iff its content is 1. Show that the product of two primitive polynomials is primitive. Deduce from this that the content of the product of two polynomials is the product of the content of these polynomials. Show that if K is the field of fractions of R then $K[X]$ is a gcd domain. Using this show that if R is a gcd domain then so is $R[X]$. (This is similar to the result that $R[X]$ is UFD if R is UFD.)

7. The goal of this exercise is to show that we cannot derive $(\exists x.x^2+1=0) \vee \forall x.x^2+1 \neq 0$ in the theory of discrete field (this can be interpreted as the fact that we cannot decide the irreducibility of polynomials). We consider the forcing associated to the theory of dicsrete fields where a covering of R is given by $R \rightarrow R/<a>$ and $R \rightarrow R[1/a]$. Show first that $R \Vdash \forall x.x^2+1 \neq 0$ holds iff R is the trivial ring. Show next that $R \Vdash \exists x.x^2+1=0$ iff there exists $x_1, \ldots, x_n$ in R such that $0 = (1+x_1^2)\ldots(1+x_n^2)$.

Local-global principle

1. If L is a distributive lattice we say that b is a complement of a iff $a \wedge b = 0$ and $a \vee b = 1$. Prove that if b' is also a complement of b then $b' = b$.

2. Find an example of a ring which has a lattice of ideals which is *not* distributive

3. We consider three sequences $X = (a_i)$, $Y = (b_j)$, $Z = (c_k)$ in a ring R connected by $c_k = \Sigma_{i+j=k} a_i b_j$. This can be written as $\Sigma c_k X^k = PQ$ where $P = \Sigma a_i X^i$ and $Q = \Sigma b_j X^j$. The following is a classical proof that if a_i and b_j are unimodular then so is c_k. We consider an arbitrary prime ideal $\mathfrak{p}$. Show that if P and Q are not 0 mod. $\mathfrak{p}$ then PQ is not 0 mod. $\mathfrak{p}$ and conclude by using the fact that a sequence is unimodular iff it is not 0 mod. any prime ideal. Read this argument in a point free way to give a proof of Gauss-Joyal identity $D(Z) = D(X) \wedge D(Y)$.

Give an example of a ring where we don't have $<Z> = <X><Y>$ (we recall that $<A>$ denotes the ideal generated by the elements of the sequence A).

If R is a domain of field of fractions K, prove that we have also $V_R(Z) = V_R(X) \wedge V_R(Y)$, where $V_R : K \to Val(K, R)$ is the space of valuations of K/R.

4. Use the previous exercise to give a constructive proof that if P in $R[X]$ is nilpotent then each coefficient of P is nilpotent.

5. Prove that $D(a + b, ab) = D(a, b)$ first by using prime ideals and then by using only the universal characterisation of the map $D : R \to Z(R)$.

6. If k is algebraically closed, show that $Zar(k[X])$ is isomorphic to the lattice of cofinite subsets of the set $k \cup \{\infty\}$.

Krull dimension

1. (Kronecker's Theorem) Implement an algorithm that given P_0, P_1, P_2, P_3 in $K[X, Y]$ compute Q_0, Q_1, Q_2 such that $V(P_0, P_1, P_2, P_3)$ the set of commun zeros of P_0, P_1, P_2, P_3 in the algebraic closure of K is equal to $V(Q_0, Q_1, Q_2)$.

2. Show that to be of Krull dimension $< n$ is a local property: if we have $a_1, \ldots, a_l$ such that $1 = D(a_1, \ldots, a_l)$ and $\mathsf{Kdim}\ R[1/a_i] < n$ for all i then we have also $\mathsf{Kdim}\ R < n$.

3. (Local Kronecker's Theorem) We say that two sequences $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are *disjoint* iff we have

$$D(a_1 b_1) = 0,\ D(a_2 b_2) \leqslant D(a_1, b_1), \ldots,\ D(a_n b_n) \leqslant D(a_{n-1}, b_{n-1})$$

Show that in this case we have

$$D(a_1, \ldots, a_k, b_1, \ldots, b_k, a_{k+1} b_{k+1}) = D(a_1 + b_1, \ldots, a_k + b_k)$$

for all $k < n$. Use this to show that if R is a local ring residually discrete of Krull dimension n such that its maximal ideal is finitely radically generated, then the maximal ideal can be radically generated by n elements.

Exercises on Prüfer Domain

1. Given an algorithm which witnesses

$$\forall x\ y. \exists u\ v\ w.\ \ xu = yv \wedge y(1 - u) = xw$$

we can compute an inverse of any ideal generated by two elements. Compute from this the inverse of an arbitrary finitely generated ideal (hint: given a finite sequence of elements, show that, locally, one element divides all the others)

2. Show that $\mathbb{Q}[x, y]$ defined by $y^2 = x^3$ is not a Prüfer domain.

3. Compute an inverse of the ideal $<x, y>$ in the ring $\mathbb{Q}[x, y]$ with $y^2 = 1 - x^4$