Prüfer domain

June 23, 2010

We consider *integral* domain. They are rings R with a *decidable equality* and such that $ab = 0$ implies $a = 0$ or $b = 0$. Equivalently, they are the subrings of field, where a field is a ring with a decidable equality satisfying

$$a = 0 \vee \exists b.\ ab = 1$$

and $1 \neq 0$. If K is a field, it is decidable whether an element a in K is invertible or not.

It may be convenient to formalize the notion of field as a ring with a decidable equality and a function inv such that $a\ inv(a) = 1$ whenever $a \neq 0$, and taking $inv(0) = 0$.

Given a ring R one important problem we want to study is how to solve *linear systems* over R. Given a rectangular matrix M over R we want to find a finite number of solutions $X_1, \ldots, X_n$ of the system $MX = 0$ such that *any* solution is of the form $a_1X_1 + \ldots + a_nX_n$. We say that the module of solutions of the system $MX = 0$ is *finitely generated*.

We can reformulate this with matrices. What we ask is to find a matrix L such that $ML = 0$ and

$$MX = 0 \quad \leftrightarrow \quad \exists Y.\ X = LY$$

A ring is *coherent* iff for any matrix M, we can find a matrix L such that this implication holds.

For this, it is enough to consider the case where M has only one line. Indeed, assme that for any $1 \times n$ matrix M we can find a $n \times m$ matrix L such that $ML = 0$ and $MX = 0$ iff X is of the form LY. If we want to solve the system

$$(*) \qquad M_1X = \ldots = M_kX = 0$$

where each M_i is a $1 \times n$ matrix. We first compute L_1 such that $M_1X = 0$ iff X is of the form L_1X_1. We compute then L_2 such that $M_2L_1X_1 = 0$ iff X_1 is of the form L_2X_2. At the end we obtain $L_1, \ldots, L_k$ such that $M_1X = \ldots = M_kX = 0$ iff X is of the form $L_1 \ldots L_kY$, and so $L_1 \ldots L_k$ provide a system of generators for the system $(*)$.

Special cases: we can generate the solutions of a system $ax = 0$ (this is trivial if the ring is an integral domain), and given two finitely generated ideals $I = \langle a_1, \ldots, a_n \rangle$ and $J = \langle b_1, \ldots, b_m \rangle$ we can generate the intersection $I \cap J$. This is possible if the ring is coherent since we can look at the system

$$AX - BY = 0$$

with A is the $1 \times n$ matrix $(a_1, \ldots, a_n)$ and B is the $1 \times m$ matrix $(b_1, \ldots, b_m)$. We can find a finite number $(X_1, Y_1), \ldots, (X_p, Y_p)$ of generators. Then $AX_1, \ldots, AX_p$ generate $I \cap J$. Another system of generators is $BY_1, \ldots, BY_p$.

Conversely, assume that R is an integral domain ring such that: the intersection of two finitely generated ideal is finitely generated, then R is coherent. Then I claim that R is coherent. Indeed, consider first the system

$$ax + by = 0$$

By hypothesis we can find $t_1, \ldots, t_p$ such that

$$\langle a \rangle \cap \langle -b \rangle = \langle t_1, \ldots, t_p \rangle$$

We can then write $t_i = au_i = -bv_i$. If we have $ax + by = 0$ we can write $ax = -by$ and so

$$ax = -by = \Sigma x_i t_i$$

this implies $x = \Sigma x_i u_i$ and $y = \Sigma x_i v_i$. Hence we have (u_i, v_i) as a system of generators for the solutions of $ax + by = 0$.

Next, consider the system

$$ax + by + cz = 0$$

By hypothesis we can find $t_1, \ldots, t_p$ such that

$$\langle a \rangle \cap \langle -b, -c \rangle = \langle t_1, \ldots, t_p \rangle$$

We can then write $t_i = au_i = -bv_i - cw_i$. If we have $ax+by+cz = 0$ we can write $ax = -by-cz$ and so

$$ax = -by - cz = \Sigma x_i t_i$$

this implies $x = \Sigma x_i u_i$ and

$$b(y - \Sigma x_i v_i) + c(z - \Sigma x_i w_i) = 0$$

We can then find e_j, f_j such that $be_j + cf_j = 0$ and

$$y - \Sigma x_i v_i = \Sigma y_j e_j, \quad z - \Sigma x_i w_i = \Sigma y_j f_j$$

In this way we find the system of generators (u_i, v_i, w_i) and $(0, e_j, f_j)$.

The same argument actually shows that if R is an arbitrary ring (not necessarily an integral domain) such that: the intersection of two finitely generated ideal is finitely generated, *and* for any a the ideal $\{x \in R \mid ax = 0\}$ is finitely generated, then R is coherent.

Riesz space

The multiplicative monoid of an integral domain has the cancellation property: if $ab = ac$ then $b = c$. The structure of Riesz space plays a role both for GCD domain and for Prüfer domain, two rather different structures, and so it is nice to be explicit about this structure. One usually uses an additive notation instead of a multiplicative notation when dealing with Riesz spaces.

Let us consider a commutative monoid $M, +$ with a zero element 0 which has the cancellation property: $a + b = a + c$ implies $b = c$.

We define $a \leqslant b$ iff there exists c such that $a + c = b$. By the cancellation property $a \leqslant b$ iff $d + a \leqslant d + b$. We assume also that any two elements a and b have a meet $a \wedge b$. We write $a \perp b$ iff $a \wedge b \leqslant 0$. We have a_1 and b_1 such that $a_1 + a \wedge b = a$ and $b_1 + a \wedge b = b$. We then have $a_1 \wedge b_1 = 0$. We can then check that the element

$$a \vee b = a_1 + a \wedge b + b_1$$

is the least upper bound of a and b.

Dually, one can assume given the sup operation $a \vee b$ and since $a \vee b \leqslant a + b$ define $a \wedge b$ by

$$a \vee b + a \wedge b = a + b$$

The main Lemma is Euclide's Lemma: if $a \leqslant b + c$ and $a \perp c$ then $a \leqslant b$. This is because $a \leqslant b + a$ and so $a \leqslant b + c \wedge a = b$.

The lattice $M, \wedge, \vee$ is then automatically distributive. Furthermore $n(a \wedge b) = na \wedge nb$. Indeed, we write $a_1 + a \wedge b = a,\ b_1 + a \wedge b = b$ and we have to show $na_1 \wedge nb_1 = 0$. This follows from a direct consequence of Euclide's Lemma: if $a \perp b$ and $a \perp c$ then $a \perp b + c$. Indeed $u = a \wedge (b + c)$ satisfies $u \leqslant a$ and so $u \perp b$ and $u \perp c$. Since $u \leqslant b + c$ it follows from Euclide's Lemma that $u = 0$.

Bezout ring

A ring is a Bezout ring iff any finitely generated ideal is principal, i.e. generated by one element.

Main examples of Bezout rings are $\mathbb{Z}$ the ring of integers, and the ring $\mathbf{K}[X]$ of polynomials with one variable.

In contrast, the ring $\mathbf{K}[X, Y]$ is *not* a Bezout ring since the ideal $\langle X, Y\rangle$ cannot be generated by one element. The ring $\mathbb{Z}[X]$ is not a Bezout ring since the ideal $\langle 2, X\rangle$ cannot be generated by one element.

Both $\mathbb{Z}$ and $\mathbf{K}[X]$ are Euclidian domain: we have a norm $|a|$ and if $b \neq 0$ we can find q and r such that $a = bq + r$ and $|r| < |b|$. All we need to apply the Euclidian algorithm for computing the gcd g of a and b is then that the relation $<$ on norms is well-founded. We then have $\langle a, b\rangle = \langle g\rangle$.

GCD domain

We say that an integral domain R is a GCD domain iff two nonzero elements a and b have a gcd, i.e. an element g such that g divides a and b and such that if c divides a and b then c divides g.

A fundamental result is that if R is a GCD domain then so is $R[X]$. This implies that the rings $\mathbb{Z}[X_1, \ldots, X_n]$ and $\mathbf{K}[X_1, \ldots, X_n]$ are GCD domain.

The main Lemma in the proof of this result is Gauss Lemma. We define the *G-content* $c(P)$ of a polynomial P in $R[X]$ to be the gcd of the coefficients of P (this is well defined up to an unit of R). We say that a polynomial P is *G-primitive* iff $c(P) = 1$.

Lemma 0.1 *$c(PQ) = c(P)c(Q)$. In particular, the product of two G-primitive polynomials is G-primitive.*

Prüfer domain

The definition is very simple logically

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

What really matters is that b divides a in $R[1/u]$ and a divides b in $R[1/(1 - u)]$.

An equivalent definition is that for any elements a and b we can find $u_1, \ldots, u_n$ such that $1 = \langle u_1, \ldots, u_n\rangle$ and a divides b or b divides a on each localisation $R[1/u_i]$.

From this, it follows that for any nonzero finitely generated ideal I we can find a nonzero finitely generated ideal J such that IJ is principal.

Here is the idea of the algorithm: let $a_1, \ldots, a_n$ be (nonzero) generators of I, we can find a $n \times n$ matrix (u_{ij}) such that $\Sigma u_{ii} = 1$ and $u_{ij}a_j = u_{ii}a_i$. This matrix is called a *principal localization matrix* and can be computed for any Prüfer domain.

We get then $\langle u_{11}, \ldots, u_{n1}\rangle I = \langle a_1\rangle$

It follows that the monoid of (nonzero) finitely generated ideal has the cancellation property. Indeed, if $IJ = IK$ and I' is such that $II' = \langle a\rangle$ we get $aJ = aK$ and hence $J = K$.

An important other corollary (that was a crucial property for Dedekind) is that if $I \subseteq J$ then there exists K such that $JK = I$. For this, we compute J' such that $JJ' = \langle b\rangle$. We have then $IJ' \subseteq \langle b\rangle$ and we find K such that $bK = IJ'$. We have then $bJK = IJJ' = bI$ and hence $JK = I$. Thus the order of the monoid operation: there exists K such that $IK = J$ coincides with the inclusion ordering $J \subseteq I$.

Since we have a sup operation (the sum of two finitely generated ideal is finitely generated) we have a meet as well, and this gives an algorithm showing that in a Prüfer domain, the intersection of two finitely generated ideal is finitely generated. It follows that any Prüfer domain is *coherent*. More precisely, the algorithm for computing $I \cap J$ is the following. We have $IJ \subseteq I + J$. But the corollary we have just seen, this implies that there exists K such that $IJ = K(I + J)$. One can then show $K = I \cap J$.

Notice that $K[X, Y]$ is a gcd domain which is *not* a Prüfer domain.

Integral closure

The last step is to show that if R is a Bezout domain, of field of fraction K and L is an extension of K, then the integral closure S of R inside K (i.e. the ring of elements of L integral over R) is a Prüfer domain.

For instance, the ring $K[x, y]$ with $y^2 = 1 - x^4$ or the ring $\mathbb{Z}[\sqrt{-5}]$ are Prüfer domain, and hence are coherent. Hence we can find generators for solution of any system of homogeneous equations over these rings.

Here is the idea of the algorithm. Given a and b that are nonzero and integral over R, the element $s = b/a$ is algebraic over K and hence satisfies an equation of the form

$$a_0 s^n + a_1 s^{n-1} + \ldots + a_n = 0$$

with $a_0, \ldots, a_n$ in R. Since R is a Bezout domain, we can assume $\langle a_0, \ldots, a_n\rangle = 1$.

The main remark is that the following elements are in S (integral over R). First $a_0 s$ is in S because we have

$$(a_0 s)^n + a_1 (a_0 s)^{n-1} + \ldots + a_0^{n-1} a_n = 0$$

Hence also $a_0 s + a_1$ is in S. We can rewrite the original equation as

$$(a_0 s + a_1) s^{n-1} + \ldots + a_n = 0$$

It follows that $(a_0 s + a_1)s$ is in S. At the end, we get that

$$a_0,\ a_0 s,\ a_0 s + a_1,\ (a_0 s + a_1)s,\ (a_0 s + a_1)s + a_2,\ \ldots$$

are all in S. We have in S

$$\langle a_0,\ a_0 s,\ a_0 s + a_1,\ (a_0 s + a_1)s,\ (a_0 s + a_1)s + a_2,\ \ldots\rangle = \langle a_0, a_1, \ldots\rangle = 1$$

and a divides b or b divides a on each localization $R[1/a_0],\ R[1/a_0 s],\ \ldots$ So we have shown that S is a Prüfer domain.

Strongly discrete

A very strong computational property of a ring is to be *strongly discrete*, that is, for any finitely generated ideal I, we can decide the membership in I. If the ring is strongly discrete and coherent, not only we can solve in a satisfactory way any homogeneous system $MX = 0$, but we can even solve any system $MX = A$.

For a Prüfer domain to be strongly discrete, it is enough that the divisibility relation is decidable. To decide if x is in I we compute I' such that $II' = \langle a \rangle$. We have x in I iff $\langle x \rangle \subseteq I$ iff $xI' \subseteq \langle a \rangle$ and we can decide this if we can decide when an element is divisible by a.

In this case, the equality of finitely generated ideal is decidable as well as the inclusion relation.