$h(x_i) = 0$ or $h(x_i)$ is an irreducible polynomial. By Proposition 40, the image of P_i in $S[x_i]$ will be saturated if and only if it equals $\mathcal{A} \cap S[x_i]$ where $\mathcal{A}$ is the ideal generated by P_i and $1 - at$ in $S[x_i, t]$. This latter condition can be checked in $k[x_1, \ldots, x_i, t]$: it is equivalent to checking that the intersection of the ideal generated by P_i and $1 - at$ in $k[x_1, \ldots, x_i, t]$ with $k[x_1, \ldots, x_i]$ is just P_i (cf. Exercise 3).

Combining these observations with our results on Gröbner bases from Chapter 9 we obtain the following algorithm for determining whether the ideal P in $k[x_1, \ldots, x_n]$ is prime (or, equivalently, whether the associated affine algebraic set is a variety).

Algorithm for Determining when an Ideal in $k[x_1, \ldots, x_n]$ is Prime

(1) Compute the reduced Gröbner basis $G = \{g_1, \ldots, g_m\}$ for P with respect to the lexicographic monomial ordering $x_n > \cdots > x_1$.

By Proposition 29 in Section 9.6 the elements of G lying in $k[x_1, \ldots, x_i]$ will be the reduced Gröbner basis $\{g_1, \ldots, g_{m_i}\}$ for $P_i = P \cap k[x_1, \ldots, x_i]$.

(2) Determine whether P_1 is a prime ideal in $k[x_1]$ by checking that $P_1 = 0$ or the nonzero generator of P_1 is irreducible in $k[x_1]$.

For each $i \geq 2$, suppose P_{i-1} has been determined to be a prime ideal in $k[x_1, \ldots, x_{i-1}]$ (otherwise, P is not a prime ideal in $k[x_1, \ldots, x_n]$). Let $S = k[x_1, \ldots, x_{i-1}]/P_{i-1}$ and let F be the fraction field of S. Apply steps (3) and (4) to determine whether P_i is a prime ideal in $k[x_1, \ldots, x_i]$.

(3) If $m_i = m_{i-1}$ then P_i maps to the zero ideal in $S[x_i]$, hence is prime. Otherwise the image of P_i in $S[x_i]$ and in $F[x_i]$ is a nonzero ideal, and is generated by the images of $g_{m_{i-1}+1}, \ldots, g_{m_i}$. Apply the Euclidean algorithm in $F[x_i]$ to these generators to find an element $h(x_i)$ in P_i whose image in $F[x_i]$ generates the image of P_i in $F[x_i]$. Determine whether $h(x_i)$ is irreducible in $F[x_i]$—if not then P_i and P are not prime ideals.

(Note that after applying the Euclidean algorithm to the generators of the image of P_i in $F[x_i]$ we can multiply by a single element of S to 'clear denominators' in each equation so that all remainders (and in particular the last nonzero remainder $h(x_i)$) will be elements in the image of P_i.)

(4) Let $a \in k[x_1, \ldots, x_{i-1}]$ be the leading coefficient of $h(x_i)$ (as a polynomial in x_i). Compute the reduced Gröbner basis in $k[x_1, \ldots, x_i, t]$ for the ideal generated by P_i and $1 - at$ with respect to the lexicographic monomial ordering $t > x_i > \cdots > x_1$. Determine whether the elements of this reduced basis that lie in $k[x_1, \ldots, x_i]$ are $\{g_1, \ldots, g_{m_i}\}$—if so, then P_i is a prime ideal in $k[x_1, \ldots, x_i]$ and if not then P_i and P are not prime ideals.

Finally, we note that similar ideas (together with some minor modifications to extend results on Gröbner bases to polynomial rings $R[x_1, \ldots, x_n]$ with coefficients in an integral domain R) can be used to provide algorithms for determining when an ideal in, for example, $\mathbb{Z}[x_1, \ldots, x_n]$ is prime.

Examples

(1) Consider the ideal $P = (xz - y^2, yz - x^3, z^2 - x^2y)$ in $k[x, y, z]$ for any infinite field k. It follows from Exercise 26 in Section 1 that P is a prime ideal since there is an injection of $k[x, y, z]/P$ into the integral domain $k[\mathbb{A}^1]$ (cf. Exercise 24 in Section 2). Here we prove $P \subset \mathbb{Q}[x, y, z]$ is prime using the ideas in this section. The reduced Gröbner basis for P with respect to the lexicographic monomial ordering $x > y > z$ is $\{x^3 - yz, x^2y - z^2, xy^3 - z^3, xz - y^2, y^5 - z^4\}$. Hence $P_1 = P \cap \mathbb{Q}[z] = (0)$, and $P_2 \cap \mathbb{Q}[y, z] = (y^5 - z^4)$. Since $P_1 = 0$, the ideal P_1 is prime in $\mathbb{Q}[z]$.

We next check P_2 is prime in $\mathbb{Q}[y, z]$, which can be done directly (cf. Exercise 4 or Exercise 14 in Section 9.1). In this case $S = \mathbb{Q}[z]$ and $F = \mathbb{Q}(z)$. The image of P_2 in $F[y]$ is generated by $h(y) = y^5 - z^4$, which is irreducible in $\mathbb{Q}(z)[y]$. The leading coefficient of $h(y)$ is 1, and the reduced Gröbner basis for $(y^5 - z^4, 1 - t)$ in $\mathbb{Q}[y, z, t]$ with respect to the lexicographic monomial ordering $t > y > z$ is $\{y^5 - z^4, 1 - t\}$. The element in the reduced Gröbner basis for P_2 is the only element of this basis lying in $\mathbb{Q}[y, z]$ so P_2 is a prime ideal in $\mathbb{Q}[y, z]$.

We now use the fact that P_2 is prime to prove that P is prime. In this case S is the integral domain $\mathbb{Q}[y, z]/P_2 = \mathbb{Q}[y, z]/(y^5 - z^4)$ with quotient field F given by

$$S = \mathbb{Q}[\bar{z}] + \mathbb{Q}[\bar{z}]\bar{y} + \mathbb{Q}[\bar{z}]\bar{y}^2 + \mathbb{Q}[\bar{z}]\bar{y}^3 + \mathbb{Q}[\bar{z}]\bar{y}^4$$

$$F = \mathbb{Q}(\bar{z}) + \mathbb{Q}(\bar{z})\bar{y} + \mathbb{Q}(\bar{z})\bar{y}^2 + \mathbb{Q}(\bar{z})\bar{y}^3 + \mathbb{Q}(\bar{z})\bar{y}^4$$

where $\bar{y}^5 = \bar{z}^4$. The image of P in $S[x]$ is the ideal $\overline{P}$ generated by the elements $g_1 = x^3 - \bar{y}\bar{z}$, $g_2 = \bar{y}x^2 - \bar{z}^2$, $g_3 = \bar{y}^3x - \bar{z}^3$, $g_4 = \bar{z}x - \bar{y}^2$, and $\bar{y}^5 - \bar{z}^4 = 0$.

The greatest common divisor in $F[x]$ of g_1, g_2, g_3, g_4 generating the image of P in $F[x]$ is the irreducible polynomial $x - \bar{y}^2/\bar{z}$. The polynomial $h(x) = zx - y^2$ in P has image generating the same ideal in $F[x]$, so we may take $a = z$ in (4) of the algorithm. The reduced Gröbner basis for $(xz - y^2, yz - x^3, z^2 - x^2y, 1 - zt)$ with respect to the lexicographic monomial ordering $t > x > y > z$ consists of the reduced Gröbner basis for P together with the elements $ty^2 - x$ and $tz - 1$ involving t, so P is a prime ideal in $\mathbb{Q}[x, y, z]$.

(2) Consider the ideal $P = (xz - y^3, xy - z^2)$ in $\mathbb{Q}[x, y, z]$, with reduced Gröbner basis for the lexicographic monomial ordering $x > y > z$ given by $\{xy - z^2, xz - y^3, y^4 - z^3\}$. Here $P_1 = 0$ and $P_2 = P \cap \mathbb{Q}[y, z] = (y^4 - z^3)$ are prime ideals as in Example 1. In this case $S = \mathbb{Q}[y, z]/P_2$ is given by

$$S = \mathbb{Q}[\bar{z}] + \mathbb{Q}[\bar{z}]\bar{y} + \mathbb{Q}[\bar{z}]\bar{y}^2 + \mathbb{Q}[\bar{z}]\bar{y}^3$$

with $\bar{y}^4 = \bar{z}^3$, with quotient field F similar to the previous example, and $\overline{P} = (g_1, g_2)$ in $S[x]$ where $g_1 = \bar{y}x - \bar{z}^2$ and $g_2 = \bar{z}x - \bar{y}^3$. The extension of $\overline{P}$ to $F[x]$ is generated by the irreducible polynomial $\bar{y}x - \bar{z}^2$, and $h(x) = yx - z^2$ is an element of P having the same image in $F[x]$, with leading coefficient $a = y$. The reduced Gröbner basis for the ideal $(xz - y^3, xy - z^2, 1 - yt)$ in $\mathbb{Q}[x, y, z, t]$ using the lexicographic ordering $t > x > y > z$ is $\{x^2 - y^2z, xy - z^2, xz - y^3, y^4 - z^3, ty - 1, tz^2 - x\}$, containing the element $x^2 - y^2z$ not in the reduced Gröbner basis for P, so P is *not* a prime ideal in $\mathbb{Q}[x, y, z]$. This computation not only shows P is not a prime ideal, it does so by explicitly showing the image of P in $S[x]$ is not saturated using the localization S_a. The computation of $a = y$ allows us to find an explicit pair of elements not in P whose product is in P: $f = x^2 - y^2z \notin P$ and $y \notin P$, but some power of y times f lies in P. In this case a quick computation verifies that $yf \in P$.

Localizations of Modules

Suppose now that M is an R-module and D is a multiplicatively closed subset of R containing 1 as above. Then the ideas used in the construction of $D^{-1}R$ can be used to construct a $D^{-1}R$-module $D^{-1}M$ from M in a similar fashion, as follows. Define the relation on $D \times M$ by

$$(d, m) \sim (e, n) \quad \text{if and only if} \quad x(dn - em) = 0 \quad \text{for some } x \in D,$$

which is easily checked to be an equivalence relation. Let m/d denote the equivalence class of (d, m) and let $D^{-1}M$ denote the set of equivalence classes. It is then straightforward to verify that the operations

$$\frac{m}{d} + \frac{n}{e} = \frac{em + dn}{de} \qquad \text{and} \qquad \left(\frac{r}{d}\right)\left(\frac{m}{e}\right) = \frac{rm}{de}$$

are well defined and give $D^{-1}M$ the structure of a $D^{-1}R$-module.

Definition. The $D^{-1}R$-module $D^{-1}M$ is called the *module of fractions of M with respect to D* or the *localization of M at D*.

Note that the localization $D^{-1}M$ is also an R-module (since each $r \in R$ acts by $r/1$ on $D^{-1}M$), and there is an R-module homomorphism

$$\pi : M \to D^{-1}M \quad \text{defined by} \quad \pi(m) = \frac{m}{1}.$$

It follows directly from the definition of the equivalence relation that

$$\ker \pi = \{m \in M \mid dm = 0 \text{ for some } d \in D\}.$$

The homomorphism π has a universal property analogous to that in Theorem 36. Suppose N is an R-module with the property that left multiplication on N by d is a bijection of N for every $d \in D$. If $\psi : M \to N$ is any R-module homomorphism then there is a unique R-module homomorphism $\Psi : D^{-1}M \to N$ such that $\Psi \circ \pi = \psi$.

If M and N are R-modules and $\varphi : M \to N$ is an R-module homomorphism, then for any multiplicative set D in R it is easy to check that there is an induced $D^{-1}R$-module homomorphism from $D^{-1}M$ to $D^{-1}N$ defined by mapping m/d to $\varphi(m)/d$.

The next result shows that the localization of M at D is related to the tensor product.

Proposition 41. Let D be a multiplicatively closed subset of R containing 1 and let M be an R-module. Then $D^{-1}M \cong D^{-1}R \otimes_R M$ as $D^{-1}R$-modules, i.e., $D^{-1}M$ is the $D^{-1}R$-module obtained by extension of scalars from the R-module M.

Proof: The map from $D^{-1}R \times M$ to $D^{-1}M$ defined by mapping $(r/d, m)$ to rm/d is well defined and R-balanced, so induces a homomorphism from $D^{-1}R \otimes_R M$ to $D^{-1}M$. The map sending m/d to $(1/d) \otimes m$ gives a well defined inverse homomorphism (if $m/d = m'/d'$ in $D^{-1}M$ then $x(d'm - dm') = 0$ for some $x \in D$, and then $(1/d) \otimes m$ can be written as $(1/xd'd) \otimes (xd'm) = (1/xd'd) \otimes (xdm') = (1/d') \otimes m'$). Hence $D^{-1}M$ is isomorphic to $D^{-1}R \otimes_R M$ as an R-module since these inverse isomorphisms are also $D^{-1}R$-module homomorphisms.

Localizing a ring R or an R-module M at D behaves very well with respect to algebraic operations on rings and modules, as the following proposition shows: