as polynomials in R, where $a_1, \ldots, a_n, b_1, \ldots, b_s \in R$. Substituting $y_i = \varphi_i$ we see that $f(\varphi_1, \ldots, \varphi_m)$ is an element of I. Since $\Phi(\bar{f}) = f(\varphi_1, \ldots, \varphi_m)$ modulo I, it follows that f represents a coset in the kernel of Φ. Conversely, suppose $f \in k[y_1, \ldots, y_m]$ represents an element in $\ker \Phi$. Then $f(\varphi_1, \ldots, \varphi_m) \in I$ (in $k[x_1, \ldots, x_n]$) and so also $f(\varphi_1, \ldots, \varphi_m) \in \mathcal{A}$ (in R). Since $y_i - \varphi_i \in \mathcal{A}$,

$$f(y_1, \ldots, y_m) \equiv f(\varphi_1, \ldots, \varphi_m) \equiv 0 \bmod \mathcal{A}$$

so $f \in \mathcal{A} \cap k[y_1, \ldots, y_m]$.

For (b), suppose first that $f \in k[x_1, \ldots, x_n]$ represents an element in the image of Φ, i.e., $\bar{f} = \Phi(\bar{h})$ for some polynomial $h \in k[y_1, \ldots, y_m]$. Then

$$f(x_1, \ldots, x_n) - h(\varphi_1, \ldots, \varphi_m) \in I$$

as polynomials in $k[x_1, \ldots, x_n]$, and so $f(x_1, \ldots, x_n) - h(\varphi_1, \ldots, \varphi_m) \in \mathcal{A}$ as polynomials in R. As before, since each $y_i - \varphi_i \in \mathcal{A}$ it follows that

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) \in \mathcal{A}.$$

Then $f(x_1, \ldots, x_n)$ and $h(y_1, \ldots, y_m)$ leave the same remainder after general polynomial division by the elements in G. Since $x_1 > \cdots > x_n > y_1 > \cdots > y_m$, the remainder of $h(y_1, \ldots, y_m)$ is again a polynomial h_0 only involving $y_1, \ldots, y_m$. Note also that $h - h_0 \in \mathcal{A} \cap k[y_1, \ldots, y_m]$ so $\bar{h}$ and $\overline{h_0}$ differ by an element in $\ker \Phi$ by (a), so $\Phi(\overline{h_0}) = \Phi(\bar{h}) = \bar{f}$. For the converse, if f leaves the remainder $h \in k[y_1, \ldots, y_m]$ after general polynomial division by the elements in G then $f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) \in \mathcal{A}$, i.e.,

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) = \sum_{i=1}^{n} a_i(y_i - \varphi_i) + \sum_{j=1}^{s} b_j f_j$$

as polynomials in R, where $a_1, \ldots, a_n, b_1, \ldots, b_s \in R$. Substituting $y_i = \varphi_i$ we obtain

$$f(x_1, \ldots, x_n) - h(\varphi_1, \ldots, \varphi_m) \in I$$

as polynomials in $x_1, \ldots x_n$, and so $\bar{f} = \Phi(\bar{h})$.

It follows in particular from Proposition 8 that Φ will be a surjective homomorphism if and only if for each $i = 1, 2, \ldots, n$, dividing x_i by the elements in the Gröbner basis G leaves a remainder h_i in $k[y_1, \ldots, y_m]$. In particular, $x_n - h_n$ leaves a remainder of 0. But this means the leading term of some element g_n in G divides the leading term of $x_n - h_n$ and since $x_1 > \cdots > x_n > y_1 > \cdots > y_m$ by the choice of the ordering, the leading term of $x_n - h_n$ is just x_n. It follows that $LT(g_n) = x_n$ and so $g_n = x_n - h_{n,0} \in G$ for some $h_{n,0} \in k[y_1, \ldots, y_m]$ (in fact $h_{n,0}$ is the remainder of h_n after division by the elements in G). Next, since $x_{n-1} - h_{n-1}$ leaves a remainder of 0, there is an element g_{n-1} in G whose leading term is x_{n-1}. Since G is a reduced Gröbner basis and $g_n \in G$, the leading term of g_n, i.e., x_n, does not divide any of the terms in g_{n-1} and it follows that $g_{n-1} = x_{n-1} - h_{n-1,0} \in G$ for some $h_{n-1,0} \in k[y_1, \ldots, y_m]$. Proceeding in a similar fashion we obtain the following corollary, showing that whether Φ is surjective can be seen immediately from the elements in the reduced Gröbner basis.

Corollary 9. The map Φ is surjective if and only if for each i, $1 \leq i \leq n$, the reduced Gröbner basis G contains a polynomial $x_i - h_i$ where $h_i \in k[y_1, \ldots, y_m]$.

Examples

(1) Let $\Phi : \mathbb{Q}[u, v] \to \mathbb{Q}[x]$ be defined by $\Phi(u) = x^2 + x$ and $\Phi(v) = x^3$. The reduced Gröbner basis G for the ideal $\mathcal{A} = (u - x^2 - x, v - x^3)$ with respect to the lexicographic monomial ordering $x > u > v$ is

$$g_1 = x^2 + x - u, \qquad g_3 = vx - x - u^2 + u + 2v,$$
$$g_2 = ux + x - u - v, \qquad g_4 = u^3 - 3uv - v^2 - v.$$

The kernel of Φ is the ideal generated by $G \cap \mathbb{Q}[u, v] = \{g_4\}$. By Corollary 9, we see that Φ is not surjective. The remainder after general polynomial division of x^4 by $\{g_1, g_s, g_3, g_4\}$ is $x + u^2 - u - 2v \notin \mathbb{Q}[u, v]$, so x^4 is not in the image of Φ. The remainder of $x^5 + x$ is $-u^2 + uv + u + 2v \in \mathbb{Q}[u, v]$ so $x^5 + x = \Phi(-u^2 + uv + u + 2v)$ is in the image of Φ, as a quick check will confirm.

(2) Let $V = \mathcal{Z}(I) \subset \mathbb{C}^3$ and $W = \mathcal{Z}(J) \subset \mathbb{C}^2$ where $I = (xz + y^2 + z^2, xy - xz + yz - 2z^2)$ and $J = (u^3 - uv^2 + v^3)$ as in Example 2 following Corollary 7. Then the map $\varphi : V \to W$ defined by $\varphi((a, b, c)) = (c, b)$ is a morphism from V to W. To see this, we must check that $(c, b) \in W$ if $(a, b, c) \in V$. Equivalently, by Theorem 6, we must check that the map

$$\widetilde{\varphi} : \mathbb{C}[u, v]/(u^3 - uv^2 + v^3) \longrightarrow \mathbb{C}[x, y, z]/(xz + y^2 + z^2, xy - xz + yz - 2z^2)$$

induced by mapping u to z and v to y is a $\mathbb{C}$-algebra homomorphism. This in turn is equivalent to verifying that $f = z^3 - zy^2 + y^3$ is an element of the ideal I. In this case f is actually an element in the reduced Gröbner basis for I:

$$xy + y^2 + yz - z^2, \qquad xz + y^2 + z^2, \qquad y^3 - y^2z + z^3,$$

so certainly $f \in I$. (Note that dividing f by the original two generators for I leaves the nonzero remainder f itself, from which it is much less clear that $f \in I$, so it is important to use a Gröbner basis when working in coordinate rings.)

(3) In the previous example, let $\mathcal{A} = (u - z, v - y, xz + y^2 + z^2, xy - xz + yz - 2z^2) \subset \mathbb{C}[u, v, x, y, z]$ as in Proposition 8. With respect to the lexicographic monomial ordering $x > y > z > u > v$ the reduced Gröbner basis G for $\mathcal{A}$ is

$$xu + u^2 + v^2, \quad xv - u^2 + uv + v^2, \quad y - v, \quad z - u, \quad u^3 - uv^2 + v^3.$$

By Proposition 8, we see that $\ker \widetilde{\varphi}$ is generated by $u^3 - uv^2 + v^3 \equiv 0 \bmod J$, so $\widetilde{\varphi}$ is injective. Since there is no element of the form $x - h(u, v)$ in G, $\widetilde{\varphi}$ is not surjective (in fact x is not in the image).

As a final example, we use the determination of the kernel of k-algebra homomorphisms to compute minimal polynomials of elements in simple algebraic field extensions.

Proposition 10. Suppose α is a root of the irreducible polynomial $p(x) \in k[x]$ and $\beta \in k(\alpha)$, say $\beta = f(\alpha)$ for the polynomial $f \in k[x]$. Let G be the reduced Gröbner basis for the ideal $(p, y - f)$ in $k[x, y]$ for the lexicographic monomial ordering $x > y$. Then the minimal polynomial of β over k is the monic polynomial in $G \cap k[y]$.

Proof: The kernel of the k-algebra homomorphism $k[y] \to k[x]/(p) \cong k(\alpha)$ defined by mapping y first to f and then to β is the principal ideal generated by the minimal polynomial of β in $k[y]$, and the result follows by Proposition 8.

Example

Take $k = \mathbb{Q}$, and let $\beta = 1 + \sqrt[3]{2} + 3\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$. Then the ideal $(x^3 - 2, y - (1 + x + 3x^2))$ in $\mathbb{Q}[x, y]$ has reduced Gröbner basis $\{53x - 3y^2 + 7y + 32, y^3 - 3y^2 - 15y - 93\}$ for the lexicographic monomial ordering $x > y$, so the minimal polynomial for β is $y^3 - 3y^2 - 15y - 93$.

EXERCISES

Let R be a commutative ring with $1 \neq 0$ and let k be a field.

1. Prove the converse to Hilbert's Basis Theorem: if the polynomial ring $R[x]$ is Noetherian, then R is Noetherian.
2. Show that each of the following rings are not Noetherian by exhibiting an explicit infinite increasing chain of ideals:
   (a) the ring of continuous real valued functions on [0, 1],
   (b) the ring of all functions from any infinite set X to $\mathbb{Z}/2\mathbb{Z}$.
3. Prove that the field $k(x)$ of rational functions over k in the variable x is not a finitely generated k-algebra. (Recall that $k(x)$ is the field of fractions of the polynomial ring $k[x]$. Note that $k(x)$ *is* a finitely generated *field extension* over k.)
4. Prove that if R is Noetherian, then so is the ring $R[[x]]$ of formal power series in the variable x with coefficients from R (cf. Exercise 3, Section 7.2). [Mimic the proof of Hilbert's Basis Theorem.]
5. (*Fitting's Lemma*) Suppose M is a Noetherian R-module and $\varphi : M \to M$ is an R-module endomorphism of M. Prove that $\ker(\varphi^n) \cap \text{image}(\varphi^n) = 0$ for n sufficiently large. Show that if φ is surjective, then φ is an isomorphism. [Observe that $\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \ldots$.]
6. Suppose that $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is an exact sequence of R-modules. Prove that M is a Noetherian R-module if and only if M' and M'' are Noetherian R-modules.
7. Prove that submodules, quotient modules, and finite direct sums of Noetherian R-modules are again Noetherian R-modules.
8. If R is a Noetherian ring, prove that M is a Noetherian R-module if and only if M is a finitely generated R-module. (Thus any submodule of a finitely generated module over a Noetherian ring is also finitely generated.)
9. For k a field show that any subring of the polynomial ring $k[x]$ containing k is Noetherian. Give an example to show such subrings need not be U.F.D.s. [If $k \subset R \subseteq k[x]$ and $y \in R - k$ show that $k[x]$ is a finitely generated $k[y]$-module; then use the previous two exercises. For the second, consider $k[x^2, x^3]$.]
10. Prove that the subring $k[x, x^2y, x^3y^2, \ldots, x^iy^{i-1}, \ldots]$ of the polynomial ring $k[x, y]$ is *not* a Noetherian ring, hence not a finitely generated k-algebra. (Thus subrings of Noetherian rings need not be Noetherian and subalgebras of finitely generated k-algebras need not be finitely generated.)
11. Suppose R is a commutative ring in which all the prime ideals are finitely generated. This exercise proves that R is Noetherian.