15.1 Suggested Problems

Problems 47 and 48

Nitesh Mathur
Ryan Kinser

March 16, 2021

Table of Contents

15.1.47

- Define $\Phi : \mathbb{Q}[u, v, w] \to \mathbb{Q}[x, y]$ by $\Phi(u) = x^2 + y^2, \Phi(v) = x + y^2$, and $\Phi(w) = x - y$. Show that neither x nor y is in the image of Φ. Show that $f = 2x^3 - 4xy - 2y^3 - 4y$ is in the image of Φ and find a polynomial in $\mathbb{Q}[u, v, w]$ mapping to f. Show that $\ker \Phi$ is the ideal generated by

$$u^2 - 2uv - 2uw^2 + 4uw + v^2 - 2vw^2 - 4vw + w^4 + 3w^2$$

Notations

- Let $\Phi : k[y_1, ..., y_m]/J \to k[x_1, ..., x_n]/I$, where $I - \mathcal{I}(V), J = \mathcal{I}(W)$ are ideals and $V \subset \mathcal{A}^n, W \subset \mathcal{A}^m$.
- For $1 \leq i \leq m$, let $\phi_i \in k[x_1, ..., x_n]$ be any polynomial representing the coset $Phi(\bar{y}_i)$.
- **Proposition 8** Let $R = k[y_1, ..., y_m, x_1, ..., x_n]$ and let $\mathcal{A}$ be the ideal generated by $y_1 - \phi_1, ..., y_m - \phi_m$ together with generators for I. Let G be the reduced Gröbner asis of $\mathcal{A}$ with respect to the lexicogrpahic monomial ordering $x_1 > ... > x_n > y_1 > ... > y_,$. Then,

Definitions and Theorems

- (a) The kernel of Φ is $\mathcal{A} \cap k[y_1, ..., y_m]$ modulo J. The elements of G in $k[y_1, .., y_m]$ (taken modulo J) generate $\ker \Phi$.
- (b) If $f \in k[x_1, .., x_n]$ then $\bar{f}$ is in the image of Φ iff the remainder after the general polynomial division of f by the elements in G is an element $h \in k[y_1, ..., y_m]$, in which case $\Phi(\bar{h}) = \bar{f}$.
- **Corollary 9** The map Φ is surjective iff for each $i, 1 \leq i \leq n$, the reduced Gröbner basis G contains a polynomial $x_i - h_i$ where $h_i \in k[y_1, ..., y_m]$.

Solution

- Let $k = \mathbb{Q}$.
- Consider the Gröbner basis generated by $(u - (x^2 + y^2), v - (x + y^2), w - (x - y))$.
- $$\begin{aligned} g_1 &= u^2 - 2uv + v^2 + 4uw - 4vw + 3w^2 - 2uw^2 - 2vw^2 + w^4 \\ g_2 &= -u + v - w + w^2 + 2wy \\ g_3 &= 3u - 3v + 3w - uw - 3vw + w^3 + 2uy - 2vy \\ g_4 &= -v + w + y + y^2 \\ g_5 &= -w + x - y \end{aligned}$$
- The kernel of Φ is the ideal generated by $G \cap \mathbb{Q}[u, v, w] = \{g_1\}$ by Proposition 8.

Table of Contents

15.1.48

- Suppose α is a root of the irreducible polynomial $p(x) \in k[x]$ and $\beta = f(\alpha)/g(\alpha)$ with polynomials $f(x), g(x) \in k[x]$ with $g(\alpha) \neq 0$.
  (a) Show $ag + bp = 1$ for some polynomials $a, b \in k[x]$ and show $\beta = h(\alpha)$ where $h = af$.
  (b) Show that the ideals $(p, y - h)$ and $(p, gy - f)$ are equal in $k[x, y]$.
  (c) Conclude that the minimal polynomial for β is the monic polynomial in $G \cap k[y]$ where G is the reduced Gröbner basis for the ideal $(p, , gy - f)$ in $k[x, y]$ for the lexicographic monomial ordering $x > y$.
  (d) Find the minimal polynomial over $\mathbb{Q}$ of $(3 - \sqrt[3]{2} + \sqrt[3]{4})/(1 + 3\sqrt[3]{2} - 3\sqrt[3]{4})$.

Definitions and Theorems

- An integral domain in which every ideal (a, b) generated by two elements is principal is called a *Bezout Domain*.
- (Exercise 8.2.7) An integral domain R is a Bezout Domain iff every pair of elements a, b of R has a gcd in R that can be written as an R-linear combination of a and b, i.e. $d = ax + by$ for some $x, y \in R$.
- **Proposition 10** Suppose α is a root of the irreducible polynomial $p(x) \in k[x]$ and $\beta \in k(\alpha)$ and $\beta = f(\alpha)$ for the polynomial $f \in k[x]$. Let G be the reduced Groebner 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 $G \cap k[y]$.

Solution (a)

- Since α is a root of irreducible polynomial $p(x), p(\alpha) = 0$.
- We also know that $g(\alpha) \neq 0$, so if we try to reduce $g(x)$, it will not contain common factors with $p(x)$.
- So, $\gcd(p(x), g(x)) = 1$.
- By Bezout's Identity (8.2.7), there exists $a(x), b(x) \in k[x]$ such that $a(x)p(x) + b(x)g(x) = 1$.
- It follows that:

$$ag = 1 - bp$$

$$g = \frac{1 - bp}{a}$$

$$g(\alpha) = \frac{1 - b(\alpha)\underbrace{p(\alpha)}_{} = 0}{a(\alpha)}$$

Continued

- $$\beta = \frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)}{\frac{1}{a(\alpha)}} = \underbrace{f(\alpha) \cdot a(\alpha)}_{h(\alpha)}$$

Solution to (b)

- We will use part (a) for this.
- $$\begin{aligned} gy - 1 \cdot f &= gy - (ag + bp) \cdot f \\ &= gy - agf - bpf \\ &= g(y - af) - bf(p) \\ &\in (p, y - h) \end{aligned}$$
- $$\begin{aligned} y - h &= y \cdot 1 - af \\ &= y(ag + bp) - af \\ &= yag + ybp - af \\ &= yb(p) + a(gy - f) \\ &\in (p, gy - f) \end{aligned}$$

Solution to (c)

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

Solution to (d)

- Let $k = \mathbb{Q}$, $\alpha = \sqrt[3]{2}$ be the root of the irreducible polynomial $p(x) = x^3 - 2$.
- Then, $\beta = \dfrac{f(\alpha)}{g(\alpha)} = \dfrac{3 - \alpha + \alpha^2}{1 + 3\alpha - 3\alpha^2}$.
- By part (c), the minimal polynomial of β over $\mathbb{Q}$ is the monic polynomial in $G \cap \mathbb{Q}[y]$.
- Then the ideal, $(p, gy - f) = (x^3 - 2, (1 + 3x - 3x^2)y - (3 - x + x^2))$ has reduced Gröbner basis:

```
In[4]:= GroebnerBasis[{x^3 - 2, (1 + 3 x - 3 x^2) * y - 3 + x - x^2}, {x, y}]

Out[4]= {-47 - 93 y - 189 y^2 + y^3, 187 + 150 x + 377 y - 2 y^2}
```

-
- Hence, our minimal polynomial is $y^3 - 189y^2 - 93y - 47$.

The End

- Thank You!
- Questions?