

Solutions 2

P2.1. Consider the monomial ideals $I := \langle x^{u_1}, x^{u_2}, \dots, x^{u_\ell} \rangle$ and $J := \langle x^{v_1}, x^{v_2}, \dots, x^{v_m} \rangle$ in the polynomial ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$.

- i. For any monomial x^w in S , prove that the ideal $(J : x^w) := \{f \in S \mid f x^w \in J\}$ is generated by the monomials $x^{v_j} / \gcd(x^{v_j}, x^w)$ for all $1 \leq j \leq m$.
- ii. Prove that intersection $J \cap I$ is generated by monomials $\text{lcm}(x^{v_j}, x^{u_i})$ for all $1 \leq j \leq m$ and all $1 \leq i \leq \ell$.

Solution.

- i. Since the monomial $x^w x^{v_j} / \gcd(x^{v_j}, x^w)$ is clearly divisible by x^{v_j} , we have

$$\left\langle \frac{x^{v_j}}{\gcd(x^{v_j}, x^w)} \mid 1 \leq j \leq m \right\rangle \subseteq (J : x^w)$$

On the other hand, given $f \in (J : x^w)$, we have $f x^w \in J$ and each term in the product $f x^w$ is a multiply of x^{v_j} for some $1 \leq j \leq m$. Unique factorization implies that each term in f is a multiply of $x^{v_j} / \gcd(x^{v_j}, x^w)$ for some $1 \leq j \leq m$. Thus, we deduce that

$$\left\langle \frac{x^{v_j}}{\gcd(x^{v_j}, x^w)} \mid 1 \leq j \leq m \right\rangle \supseteq (J : x^w).$$

- ii. Since the monomial $\text{lcm}(x^{v_j}, x^{u_i})$ is divisible by both x^{v_j} and x^{u_i} , it lies in $J \cap I$. Conversely, suppose $f \in J \cap I$. Because $f \in J$, each term in f is a multiply of x^{v_j} for some $1 \leq j \leq m$. Similarly, we have $f \in I$ and each term in f is a multiply of x^{u_i} for some $1 \leq i \leq \ell$. Hence, the definition of the least common multiple implies that each term in f is a multiply of $\text{lcm}(x^{v_j}, x^{u_i})$ for some $1 \leq j \leq m$ and some $1 \leq i \leq \ell$. It follows that $\langle \text{lcm}(x^{v_j}, x^{u_i}) \mid 1 \leq j \leq m, 1 \leq i \leq \ell \rangle = J \cap I$. \square

P2.2. Demonstrate that the following properties uniquely determine the monomial orders $>_{\text{lex}}$ and $>_{\text{grevlex}}$ among all monomial orders $>$ on the polynomial ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ satisfying $x_1 > x_2 > \dots > x_n$.

- i. For any polynomial f in S such that $\text{LT}_{\text{lex}}(f) \in \mathbb{K}[x_i, x_{i+1}, \dots, x_n]$ for some $1 \leq i \leq n$, we have $f \in \mathbb{K}[x_i, x_{i+1}, \dots, x_n]$.
- ii. The monomial order $>_{\text{grevlex}}$ refines the partial order given by total degree and, for any homogeneous $f \in S$ such that $\text{LT}_{\text{grevlex}}(f) \in \langle x_i, x_{i+1}, \dots, x_n \rangle$ for some $1 \leq i \leq n$, we have $f \in \langle x_i, x_{i+1}, \dots, x_n \rangle$.

Solution.

- i. By definition, we have $x^u >_{\text{lex}} x^v$ if and only if there is an index $i \in \{1, 2, \dots, n\}$ such that $u_1 = v_1, u_2 = v_2, \dots, u_{i-1} = v_{i-1}$, and $u_i > v_i$. Set $x^u := \text{LM}_{\text{lex}}(f)$ and let x^v be any other monomial appearing in a polynomial f . The relation $x^u \in \mathbb{K}[x_i, x_{i+1}, \dots, x_n]$ implies that $u_1 = \dots = u_{i-1} = 0$. Since $x^u >_{\text{lex}} x^v$, it follows that $v_1 = \dots = v_{i-1} = 0$ and $x^v \in \mathbb{K}[x_i, x_{i+1}, \dots, x_n]$.

Conversely, suppose that $>$ is a monomial order on S such that the relation $\text{LT}_{>}(f) \in \mathbb{K}[x_i, x_{i+1}, \dots, x_n]$ for some $1 \leq i \leq n$ implies that $f \in \mathbb{K}[x_i, x_{i+1}, \dots, x_n]$.

Consider monomials \mathbf{x}^u and \mathbf{x}^v in S such that $\mathbf{x}^u > \mathbf{x}^v$. By setting $\mathbf{x}^w := \gcd(\mathbf{x}^u, \mathbf{x}^v)$, we have $\mathbf{x}^u = \mathbf{x}^w \mathbf{x}^{u'}$ and $\mathbf{x}^v = \mathbf{x}^w \mathbf{x}^{v'}$ where $\min(u'_j, v'_j) = 0$ for all $1 \leq j \leq n$. Since $>$ is a monomial order, it follows that $\mathbf{x}^{u'} > \mathbf{x}^{v'}$. Let i be the largest integer such that $u'_1 = u'_2 = \dots = u'_{i-1} = 0$. If $f = \mathbf{x}^{u'} - \mathbf{x}^{v'}$, then the hypothesis on $>$ implies that $v'_1 = v'_2 = \dots = v'_{i-1} = 0$. Our choice of the index i and the equation $\min(u'_i, v'_i) = 0$ imply that $u'_i > 0 = v'_i$ whence $\mathbf{x}^u >_{\text{lex}} \mathbf{x}^v$. Since \mathbf{x}^u and \mathbf{x}^v are arbitrary monomials, we conclude that $>$ equals $>_{\text{lex}}$.

- ii. By definition, we have $\mathbf{x}^u >_{\text{grevlex}} \mathbf{x}^v$ if and only if either $\deg(\mathbf{x}^u) > \deg(\mathbf{x}^v)$ or $\deg(\mathbf{x}^u) = \deg(\mathbf{x}^v)$ and there exists an index $i \in \{1, 2, \dots, n\}$ such that $u_n = v_n$, $u_{n-1} = v_{n-1}$, \dots , $u_{i+1} = v_{i+1}$, and $u_i < v_i$. Set $\mathbf{x}^w := \text{LM}_{\text{grevlex}}(f)$ and let \mathbf{x}^v be any other monomial of the same total degree appearing in a polynomial f . The relation $\mathbf{x}^u \in \langle x_i, x_{i+1}, \dots, x_n \rangle$ implies that $u_i + u_{i+1} + \dots + u_n > 0$. Since $\mathbf{x}^u >_{\text{grevlex}} \mathbf{x}^v$, we have $v_i + v_{i+1} + \dots + v_n \geq u_i + u_{i+1} + \dots + u_n > 0$ and $\mathbf{x}^v \in \langle x_i, x_{i+1}, \dots, x_n \rangle$.

Conversely, suppose that $>$ is a monomial order on S which refines total degree and, for any homogeneous polynomial f in S , the relation $\text{LT}_{>}(f) \in \langle x_i, x_{i+1}, \dots, x_n \rangle$ implies that $f \in \langle x_i, x_{i+1}, \dots, x_n \rangle$. Consider monomials \mathbf{x}^u and \mathbf{x}^v in the ring S such that $\mathbf{x}^u > \mathbf{x}^v$ and $\deg(\mathbf{x}^u) = \deg(\mathbf{x}^v)$. Setting $\mathbf{x}^w := \gcd(\mathbf{x}^u, \mathbf{x}^v)$, we have $\mathbf{x}^u = \mathbf{x}^w \mathbf{x}^{u'}$ and $\mathbf{x}^v = \mathbf{x}^w \mathbf{x}^{v'}$ where $\min(u'_j, v'_j) = 0$ for all $1 \leq j \leq n$. As $>$ is a monomial order, we see that $\mathbf{x}^{u'} > \mathbf{x}^{v'}$. Let i be the smallest integer such that $u'_n = u'_{n-1} = \dots = u'_{i+1} = 0$. If $f = \mathbf{x}^{u'} - \mathbf{x}^{v'}$, then the hypothesis on $>$ implies that $v'_1 + v'_2 + \dots + v'_i > 0$. Our choice of the index i and the equation $\min(u'_i, v'_i) = 0$ imply that $u'_i > 0 = v'_i$ whence $\mathbf{x}^u >_{\text{grevlex}} \mathbf{x}^v$. Since \mathbf{x}^u and \mathbf{x}^v are arbitrary monomials, we conclude that $>$ equals $>_{\text{grevlex}}$. \square

P2.3. Let \mathbf{M} be an $(m \times n)$ -matrix with nonnegative real entries and let r_1, r_2, \dots, r_m denote the rows of \mathbf{M} . Assume that $\text{Ker}(\mathbf{M}) \cap \mathbb{Z}^n = \{0\}$. Define a binary relation $>_{\mathbf{M}}$ on the monomials in the polynomial ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ as follows:

$\mathbf{x}^u >_{\mathbf{M}} \mathbf{x}^v$ if there is an positive integer i (at most m) such that $u \cdot r_i > v \cdot r_i$ and $u \cdot r_j = v \cdot r_j$ for all $1 \leq j \leq i - 1$.

- i. Show that $>_{\mathbf{M}}$ is a monomial order on the polynomial ring S .
- ii. When $\mathbf{M} := \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, show that $>_{\mathbf{M}}$ equals $>_{\text{grevlex}}$ on $\mathbb{K}[x, y, z]$.
- iii. For the $(n \times n)$ -identity matrix \mathbf{I} , show that $>_{\text{lex}}$ equals $>_{\mathbf{I}}$.

Solution.

- i. We check the three defining properties of a monomial order.
(total order) Suppose that \mathbf{u} and \mathbf{v} are distinct vectors in \mathbb{N}^n . Since we know that $\text{Ker}(\mathbf{M}) \cap \mathbb{Z}^n = \{0\}$, there exists a positive integer i such that $(\mathbf{u} - \mathbf{v}) \cdot r_j = 0$ for all $1 \leq j \leq i - 1$, and $(\mathbf{u} - \mathbf{v}) \cdot r_i \neq 0$. When $(\mathbf{u} - \mathbf{v}) \cdot r_i > 0$, we have $\mathbf{x}^u >_{\mathbf{M}} \mathbf{x}^v$ and otherwise $\mathbf{x}^v >_{\mathbf{M}} \mathbf{x}^u$. Therefore, the binary relation $>_{\mathbf{M}}$ is a total order on \mathbb{N}^n .

(multiplicative) Suppose that $\mathbf{x}^u >_{\mathbf{M}} \mathbf{x}^v$. By definition, there exists a positive integer i such that $\mathbf{u} \cdot \mathbf{r}_i = \mathbf{v} \cdot \mathbf{r}_j$ for all $1 \leq j \leq i-1$ and $\mathbf{u} \cdot \mathbf{r}_i > \mathbf{v} \cdot \mathbf{r}_i$. Since $\mathbf{x}^w \mathbf{x}^u = \mathbf{x}^{w+u}$ and $\mathbf{x}^w \mathbf{x}^v = \mathbf{x}^{w+v}$, it follows that $(\mathbf{w} + \mathbf{u}) \cdot \mathbf{r}_j = (\mathbf{w} + \mathbf{v}) \cdot \mathbf{r}_j$ for all $1 \leq j \leq i-1$ and $(\mathbf{w} + \mathbf{u}) \cdot \mathbf{r}_i > (\mathbf{w} + \mathbf{v}) \cdot \mathbf{r}_i$ which implies that $\mathbf{x}^w \mathbf{x}^u >_{\mathbf{M}} \mathbf{x}^w \mathbf{x}^v$.

(artinian) Let e_1, e_2, \dots, e_n be the standard basis of \mathbb{Z}^n , so $x_j = \mathbf{x}^{e_j}$ for all $1 \leq j \leq n$. Since we have $\text{Ker}(\mathbf{M}) \cap \mathbb{Z}^n = \{0\}$, there exists a positive integer i (for each e_k) such that $e_k \cdot \mathbf{r}_j = 0$ for all $1 \leq j \leq i-1$ and $e_k \cdot \mathbf{r}_j \neq 0$. Because \mathbf{M} has nonnegative entries, we have $e_k \cdot \mathbf{r}_i > 0$. Therefore, we see that $x_k >_{\mathbf{M}} 1$ for all $1 \leq k \leq n$.

ii. We have

$$\begin{aligned} x^{u_1}y^{u_2}z^{u_3} >_{\mathbf{M}} x^{v_1}y^{v_2}z^{v_3} &\iff \begin{cases} u_1 + u_2 + u_3 > v_1 + v_2 + v_3 \\ \text{or} \left\{ \begin{array}{l} u_1 + u_2 + u_3 = v_1 + v_2 + v_3 \\ u_1 + u_2 > v_1 + v_2 \end{array} \right. \\ \text{or} \left\{ \begin{array}{l} u_1 + u_2 + u_3 = v_1 + v_2 + v_3 \\ u_1 + u_2 = v_1 + v_2 \\ u_1 > v_1 \end{array} \right. \end{cases} \\ &\iff \begin{cases} u_1 + u_2 + u_3 > v_1 + v_2 + v_3 \\ \text{or} \left\{ \begin{array}{l} u_1 + u_2 + u_3 = v_1 + v_2 + v_3 \\ u_3 < v_3 \end{array} \right. \\ \text{or} \left\{ \begin{array}{l} u_1 + u_2 + u_3 = v_1 + v_2 + v_3 \\ u_3 = v_3 \\ u_2 < v_2 \end{array} \right. \end{cases} \\ &\iff x^{u_1}y^{u_2}z^{u_3} >_{\text{grevlex}} x^{v_1}y^{v_2}z^{v_3}. \end{aligned}$$

iii. We have

$$\begin{aligned} \mathbf{x}^u >_{\mathbf{I}} \mathbf{x}^v &\iff \text{there exist } i \text{ such that } u_j = v_j \text{ for all } 1 \leq j \leq i-1 \text{ and } u_i > v_i \\ &\iff \mathbf{x}^u >_{\text{lex}} \mathbf{x}^v. \end{aligned} \quad \square$$

P2.4. Let \mathbb{F}_2 be a finite field with 2 elements and consider the ideal I in $\mathbb{F}_2[x, y, z]$ consisting of all polynomials that vanish at every point in $\mathbb{A}^3(\mathbb{F}_2)$.

i. Show that $\langle x^2 - x, y^2 - y, z^2 - z \rangle \subseteq I$.

ii. For any coefficients a_0, a_1, \dots, a_7 in \mathbb{F}_2 , show that the polynomial

$$f := a_0 xyz + a_1 xy + a_2 xz + a_3 yz + a_4 x + a_5 y + a_6 z + a_7$$

belongs to the ideal I if and only if we have $a_0 = a_1 = \dots = a_7 = 0$.

iii. Show that $I = \langle x^2 - x, y^2 - y, z^2 - z \rangle$.

Solution.

i. Since the univariate polynomial $t^2 - t = t(t-1)$ has both 0 and 1 as roots for any $t \in \{x, y, z\}$, it follows that $\langle x^2 - x, y^2 - y, z^2 - z \rangle \subseteq I$.

ii. When $a_0 = a_1 = \cdots = a_7 = 0$, the polynomial f is the zero polynomial which vanishes at every point. Now, suppose that f vanishes at every point in $\mathbb{A}^3(\mathbb{F}_2)$. It follows that $f(0,0,0) = a_7 = 0$, $f(1,0,0) = a_4 = 0$, $f(0,1,0) = a_5 = 0$, and $f(0,0,1) = a_6 = 0$. We deduce that $f(1,1,0) = a_1 = 0$, $f(1,0,1) = a_2 = 0$, and $f(0,1,1) = a_3 = 0$. Finally, we have $f(1,1,1) = a_0 = 0$.

iii. Fix a monomial order $>$ on $\mathbb{F}_2[x, y, z]$ and consider a polynomial g in I . The division algorithm implies that there exists polynomials $h_1, h_2, h_3 \in \mathbb{F}_2[x, y, z]$ and scalars $a_0, a_1, \dots, a_7 \in \mathbb{F}_2$ such that

$$g = h_1(x^2 - x) + h_2(y^2 - y) + h_3(z^2 - z) + a_0xyz + a_1xy + a_2xz + a_3yz + a_4x + a_5y + a_6z + a_7$$

Since part i yields $g - h_1(x^2 - x) - h_2(y^2 - y) - h_3(z^2 - z) \in I$, part ii establishes that $a_0 = a_1 = \cdots = a_7 = 0$. We conclude that $g \in \langle x^2 - x, y^2 - y, z^2 - z \rangle$ and $I = \langle x^2 - x, y^2 - y, z^2 - z \rangle$. \square

P2.5. A ring R satisfies the *artinian* if any descending sequence of ideals in R stabilizes. In other words, for any descending sequence $I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$ of ideals in R , there exists a nonnegative integer m such that $I_m = I_{m+1} = I_{m+2} = \cdots$.

- i. For any positive integer n , show that the quotient rings $\mathbb{Z}/\langle n \rangle$ and $\mathbb{K}[x]/\langle x^n \rangle$ are artinian.
- ii. Show that rings \mathbb{Z} and $\mathbb{K}[x]$ are not artinian.
- iii. Show that every prime ideal in an artinian ring is maximal.

Solution.

i. Since $\mathbb{Z}/\langle n \rangle$ has only n distinct elements, every descending chain of ideals can have at most n distinct ideals, so must stabilize.

Regarding the quotient $\mathbb{K}[x]/\langle x^n \rangle$ as \mathbb{K} -vector space, the monomials $1, x, \dots, x^{n-1}$ form a basis, so $\dim_{\mathbb{K}} \mathbb{K}[x]/\langle x^n \rangle = n$. Moreover, every ideal in $\mathbb{K}[x]/\langle x^n \rangle$ is also a \mathbb{K} -vector subspace. It follows that every descending chain of ideals can have at most $n + 1$ distinct ideals.

ii. Since $\langle 2 \rangle \supset \langle 2^2 \rangle \supset \langle 2^3 \rangle \supset \cdots$ and $\langle x \rangle \supset \langle x^2 \rangle \supset \langle x^3 \rangle \supset \cdots$ are infinite descending chains of distinct ideals in \mathbb{Z} and $\mathbb{K}[x]$ respectively, neither ring is artinian.

iii. Let I be a prime ideal in an artinian ring R . Since I is prime, the quotient ring R/I is a domain. A descending chain of ideals in the quotient ring R/I pulls back to a descending chain of ideals in R . Since R is artinian, this the chain in R stabilizes which implies that the chain in R/I also stabilizes. In other words, the quotient ring R/I is also artinian.

Let f be a nonzero element in the quotient ring R/I . Since R/I is artinian, it follows that $\langle f^m \rangle = \langle f^{m+1} \rangle$ for some positive integer m , so $f^m = g f^{m+1}$ for some $g \in R/I$. Since R/I is a domain and $f \neq 0$, we may cancel f^m from both sides of this equation to obtain $g f = 1_R$. It follows that f is a unit. Therefore, R/I is a field and I is a maximal ideal. \square