Solutions to Exercise Sheet 2

Solution 2.1. *Some proofs in lectures.*

(1) Using the binomial expansion, we have that $(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^{m+n-i} b^i$. For every term $\binom{m+n}{i} a^{m+n-i} b^i$, if $i \leqslant n$, then this term has a factor a^m, hence this term is in I; if $i \geqslant n$, then this term has a factor b^n, hence this term is also in I. Since every such term is in I, it follows that their sum $(a+b)^{m+n} \in I$.

(2) Let $a, b \in \sqrt{I}$ and $r \in R$. By Definition 2.1 there exist some $m, n \in \mathbb{Z}_+$ such that $a^m, b^n \in I$. By part (1) we know that $(a+b)^{m+n} \in I$, hence $a+b \in \sqrt{I}$. We also have $(ra)^m = r^m a^m \in I$, hence $ra \in \sqrt{I}$. It follows that $\sqrt{I}$ is an ideal. To show that $I \subseteq \sqrt{I}$, we just need to realise that for every $a \in I$, $a^m \in I$ for $m = 1$. Hence $a \in \sqrt{I}$.

(3) Assume I is a maximal ideal in R, then R/I is a field by Proposition 2.12 (1). Since every field is an integral domain, R/I is an integral domain. By Proposition 2.12 (1) again we conclude that I is a prime ideal in I.

Assume J is a prime ideal. For any $a \in \sqrt{J}$, there exists some $n \in \mathbb{Z}_+$, such that $a^n \in J$. We claim that $a \in J$. This can be shown by induction on n. When $n = 1$, $a \in J$ is automatic. Assume $a^n \in J$ implies $a \in J$. If we have $a^{n+1} = a \cdot a^n \in J$, then either $a \in J$ or $a^n \in J$. In either case we have $a \in J$. This shows that $\sqrt{J} \subseteq J$. By part (2) we also have $J \subseteq \sqrt{J}$. It follows that $J = \sqrt{J}$, hence J is a radical ideal.

Solution 2.2. *Examples of radical and prime ideals.*

(1) Assume (f) is a prime ideal. Since $(f) \neq \Bbbk[x_1, \cdots, x_n]$, f is not a constant polynomial. If f is not an irreducible polynomial, then assume $f = f_1 f_2$ for some non-constant polynomials f_1 and f_2. Since $f_1 f_2 = f \in (f)$, it follows that either $f_1 \in (f)$ or $f_2 \in (f)$. If $f_1 \in (f)$, then $f_1 = f \cdot g_1$ for some non-zero polynomial g_1. Then $f = f_1 f_2 = f g_1 f_2$ which implies $g_1 f_2 = 1$. Hence f_2 must be a constant, which is a contradiction. If $f_2 \in (f)$, the same argument implies f_1 is a constant, which is also a contradiction. This proves that f is irreducible.

Now assume f is an irreducible polynomial. We need to show (f) is a prime ideal. By definition an irreducible polynomial is not a constant, hence $1 \notin (f)$ which means $(f) \neq \Bbbk[x_1, \cdots, x_n]$. Let $f_1 f_2 \in (f)$ for polynomials f_1 and f_2. Then we can write $f_1 f_2 = fg$ for some polynomial g. If $g = 0$, then either $f_1 = 0 \in (f)$ or $f_2 = 0 \in (f)$. If $g \neq 0$, then f is an irreducible factor in the factorisation of $f_1 f_2$, hence f is an irreducible factor of either f_1 or f_2. Therefore we still have $f_1 \in (f)$ or $f_2 \in (f)$. This proves that (f) is a prime ideal.

(2) We first show that $(\overline{f}) \subseteq \sqrt{(f)}$. For any $g \in (\overline{f})$, there exists some polynomial h such that $g = \overline{f}h = f_1 \cdots f_t h$. Let $m = \max\{k_1, \cdots, k_t\}$. Then $g^m = f_1^m \cdots f_t^m h^m = f \cdot f_1^{m-k_1} \cdots f_t^{m-k_t} h^m \in (f)$, hence $g \in \sqrt{(f)}$.

We prove the other inclusion $\sqrt{(f)} \subseteq (\overline{f})$. For any $g \in \sqrt{(f)}$, there exists some $m \in \mathbb{Z}_+$ such that $g^m \in (f)$, that is, $g^m = fh = f_1^{k_1} \cdots f_t^{k_t} h$ for some polynomial h. For every irreducible polynomial f_i, since f_i divides the right-hand side, it must divide the left-hand side as well, i.e., f_i divides g^m. Therefore f_i divides g for every i. It follows that each f_i appears in the factorisation of g, hence $g = f_1 \cdots f_k g' = \overline{f} g' \in (\overline{f})$.

(3) (f) is a radical ideal $\Longleftrightarrow \sqrt{(f)} = (f) \Longleftrightarrow (\overline{f}) = (f) \Longleftrightarrow \overline{f}$ and f differ by a unit in $\Bbbk[x_1, \cdots, x_n]$ (which is a non-zero constant). This holds if and only if $k_1 = \cdots = k_t = 1$; i.e. f has no repeated factors.

Solution 2.3. *Examples of maximal ideals.*

(1) We claim that every polynomial $f(x_1, \cdots, x_n) \in \Bbbk[x_1, \cdots, x_n]$ can be written in the form

$$f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + c$$

for some polynomials $g_1, \cdots, g_n \in \Bbbk[x_1, \cdots, x_n]$ and a constant $c \in \Bbbk$. There are two ways to explain it (*you can choose the one you like*). The first approach: we think of f as a polynomial in x_1 and consider the Euclidean division of f by $x_1 - a_1$. We get $f = (x_1 - a_1)g_1 + r_1$ where r_1 has degree 0 in x_1, namely, $r_1 \in \Bbbk[x_2, \cdots, x_n]$. Then we think of r_1 as a polynomial in x_2, and consider the Euclidean division of r_1 by $x_2 - a_2$, we get $r_1 = (x_2 - a_2)g_2 + r_2$ for some $r_2 \in \Bbbk[x_3, \cdots, x_n]$. Repeat this process to get

$$\begin{aligned} f &= (x_1 - a_1)g_1 + r_1 \\ &= (x_1 - a_1)g_1 + (x_2 - a_2)g_2 + r_2 \\ &= \cdots \\ &= (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + r_n \end{aligned}$$

where r_n is a constant. This justifies the claim. The second approach: we substitute $[(x_i - a_i) + a_i]$ into each occurence of x_i in f and expand the square brackets leaving the round brackets untouched. In the expansion every non-constant term has a factor of the form $(x_i - a_i)$. Then we can collect terms and write

$$f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + c$$

where c is a constant. This justifies the claim.

Now we look at the image of f under φ_p. We have $\varphi_p(f) = f(a_1, \cdots, a_n) = c$. Therefore $f \in \ker\varphi_p \Longleftrightarrow c = 0 \Longleftrightarrow f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n \Longleftrightarrow f \in (x_1 - a_1, \cdots, x_n - a_n)$. This proves that $m_p = \ker\varphi_p = (x_1 - a_1, \cdots, x_n - a_n)$.

Moreover, φ_p is surjective, because every $c \in \Bbbk$ is the image of the constant polynomial $f = c$. By the fundamental isomorphism theorem, we have

$$\Bbbk = \operatorname{im} \varphi_p = \Bbbk[x_1, \cdots, x_n]/\ker \varphi_p = \Bbbk[x_1, \cdots, x_n]/m_p.$$

Since $\Bbbk$ is a field, we know that m_p is a maximal ideal by Proposition 2.12 (1).

(2) $\mathbb{V}(m_p) = \{p\}$ is a single point set. By Proposition 2.16, there is a one-to-one correspondence between maximal ideals in $\Bbbk[x_1, \cdots, x_n]$ and points in $\mathbb{A}^n$. Since the ideals of the form m_p have exhausted all points in $\mathbb{A}^n$, they must be all maximal ideals in $\Bbbk[x_1, \cdots, x_n]$.

Solution 2.4. *A famous example: the twisted cubic.*

(1) We first show $X \subseteq \mathbb{V}(I)$. For every point $(t, t^2, t^3) \in X$, we have $y - x^2 = t^2 - t^2 = 0$ and $z - x^3 = t^3 - t^3 = 0$. We then show $\mathbb{V}(I) \subseteq X$. For every $(x, y, z) \in \mathbb{V}(I)$, we have $y - x^2 = 0$ and $z - x^3 = 0$, hence $y = x^2$ and $z = x^3$. It follows that $(x, y, z) = (x, x^2, x^3) \in X$.

(2) Consider the ring homomorphism

$$\varphi : \Bbbk[x, y, z] \longrightarrow \Bbbk[t]; \quad f(x, y, z) \longmapsto f(t, t^2, t^3).$$

By the fundamental isomorphism theorem, we have

$$\operatorname{im} \varphi \cong \Bbbk[x, y, z]/\ker \varphi.$$

We need to find out $\operatorname{im} \varphi$ and $\ker \varphi$.

We claim that φ is surjective, because for every $p(t) \in \Bbbk[t]$, it is the image of $p(x) \in \Bbbk[x, y, z]$. Therefore $\operatorname{im} \varphi = \Bbbk[t]$.

To find out $\ker \varphi$, we first claim that every $f(x, y, z) \in \Bbbk[x, y, z]$ can be written in the form

$$f = (y - x^2)g_1 + (z - x^3)g_2 + h$$

where $g_1, g_2 \in \Bbbk[x, y, z]$ and $h \in \Bbbk[x]$. To see this, there are still two methods. The first method: think of f as a polynomial in y, and consider the Euclidean division of f by $y - x^2$. There is a quotient $g_1 \in \Bbbk[x, y, z]$ and a remainder $r_1 \in \Bbbk[x, z]$. Then think of r_1 as a polynomial in z, and consider the Euclidean division of r_1 by $z - x^3$. There is a quotient $g_2 \in \Bbbk[x, y, z]$ (in fact, in $\Bbbk[x, z]$) and a remainder $h \in \Bbbk[x]$. In formulas,

$$f = (y - x^2)g_1 + r_1 = (y - x^2)g_1 + (z - x^3)g_2 + h.$$

The second method: we substitute $[(y - x^2) + x^2]$ into each occurence of y in f and substitute $[(z - x^3) + x^3]$ into each occurence of z in f. We then expand the square brackets leaving the round brackets untouched. In the expansion we collect terms with a factor $(y - x^2)$ or $(z - x^3)$, and write

$$f = (y - x^2)g_1 + (z - x^3)g_2 + h$$

where $h \in \Bbbk[x]$ does not involve y or z.

Armed with this claim, we find that the image of f under φ is given by

$$\varphi(f) = (t^2 - t^2)\varphi(g_1) + (t^3 - t^3)\varphi(g_2) + h(t) = h(t).$$

Therefore $\varphi(f) = 0 \iff h = 0 \iff f = (y - x^2)g_1 + (z - x^3)g_2 \iff f \in (y - x^2, z - x^3)$. This means $\ker \varphi = (y - x^2, z - x^3) = I$.

Therefore the fundamental isomorphism theorem yields that $\Bbbk[t] \cong \Bbbk[x, y, z]/I$.

(3) Since $\Bbbk[t]$ is an integral domain, by Proposition 2.12, we conclude that I is a prime ideal, hence a radical ideal. By part (1) and Proposition 2.9, $X = \mathbb{V}(I)$ implies that $I = \mathbb{I}(X)$. Since I is a prime ideal, Proposition 2.15 shows that X is an irreducible algebraic set, hence an affine variety.