Exercise sheet 2. Prerequisites: sections 1-8. Week 6

Q1. Consider the ideals $\mathfrak{p}_1 := (x, y)$, $\mathfrak{p}_2 := (x, z)$ and $\mathfrak{m} := (x, y, z)$ of $K[x, y, z]$, where K is a field. Show that $\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a minimal primary decomposition of $\mathfrak{p}_1 \cdot \mathfrak{p}_2$. Determine the isolated and the embedded prime ideals of $\mathfrak{p}_1 \cdot \mathfrak{p}_2$.

Solution. For future reference, note that we have

$$\mathfrak{m}^2 = ((x) + (y) + (z))^2 = (x^2, y^2, z^2, xy, xz, yz)$$

and

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 = ((x) + (y))((x) + (z)) = (x^2, xz, yx, yz).$$

We have $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2$ and that we also clearly have $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subseteq \mathfrak{m}^2$ since $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq \mathfrak{m}$. Thus we have $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \subseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$. Note that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime since the rings $K[x, y, z]/\mathfrak{p}_1 \simeq K[z]$ and $K[x, y, z]/\mathfrak{p}_2 \simeq K[y]$ are domains. Note also that $\mathfrak{m}$ is a maximal ideal, since $K[x, y, z]/\mathfrak{m} \simeq K$ is a field. Thus $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{m}^2$ is primary (see after Lemma 6.4 for the latter). The radicals of the ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{m}^2$ are $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{m}$ (see again Lemma 6.4 for the latter). These three ideals are distinct. Finally, we have $\mathfrak{p}_1 \not\supseteq \mathfrak{p}_2 \cap \mathfrak{m}^2$ (because $z^2 \notin \mathfrak{p}_1$ but $z^2 \in \mathfrak{p}_2 \cap \mathfrak{m}^2$), $\mathfrak{p}_2 \not\supseteq \mathfrak{p}_1 \cap \mathfrak{m}^2$ (because $y^2 \notin \mathfrak{p}_2$ but $y^2 \in \mathfrak{p}_1 \cap \mathfrak{m}^2$) and $\mathfrak{m}^2 \not\supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2$ (because $x \notin \mathfrak{m}^2$ but $x \in \mathfrak{p}_2 \cap \mathfrak{p}_2$). Hence if $\mathfrak{p}_1 \cdot \mathfrak{p}_2 = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ then this decomposition is indeed primary and minimal. Thus we only have to show that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$. From the above, we have to show that

$$(x, y) \cap (x, z) \cap (x^2, y^2, z^2, xy, xz, yz) \subseteq (x^2, xz, yx, yz)$$

Now note that we have $P(x, y, z) \in (x, y)$ iff $P(0, 0, z) = 0$ (because a polynomial lies in (x, y) iff it has no monomial containing only the variable z). Similarly, we have $P(x, y, z) \in (x, z)$ iff $P(0, y, 0) = 0$. Thus we have $P(x, y, z) \in (x, y) \cap (x, z)$ iff $P(0, y, 0) = P(0, 0, z) = 0$.

Now an element $Q(x, y, z)$ of $(x^2, y^2, z^2, xy, xz, yz)$ has the form

$$Q(x, y, z) = P_1(x, y, z)x^2 + P_2(x, y, z)y^2 + P_3(x, y, z)z^2 + P_4(x, y, z)xy + P_5(x, y, z)xz + P_6(x, y, z)yz.$$

and $Q(x, y, z)$ will thus lie in $(x, y) \cap (x, z)$ iff

$$Q(0, y, 0) = Q(0, 0, z) = P_2(0, y, 0) = P_3(0, 0, z) = 0.$$

In other words, the element $Q(x, y, z) \in (x^2, y^2, z^2, xy, xz, yz) = \mathfrak{m}^2$ will lie in $(x, y) \cap (x, z)$ iff $P_2(x, y, z) \in (x, z)$ and $P_3(x, y, z) \in (x, y)$. Consequently, if $Q(x, y, z) \in \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ then

$$Q(x, y, z) \in (x^2)+(x, z)(y^2)+(x, y)(z^2)+(xy)+(xz)+(yz) = (x^2, xy^2, zy^2, xz^2, yz^2, xy, xz, yz) = (x^2, xy, xz, yz) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$$

as required.

The prime ideals associated with the decomposition are $\mathfrak{p}_1 = \mathfrak{r}(\mathfrak{p}_1)$, $\mathfrak{p}_2 = \mathfrak{r}(\mathfrak{p}_2)$ and $\mathfrak{m} = \mathfrak{r}(\mathfrak{m}^2)$. The ideal $\mathfrak{m}$ contains $\mathfrak{p}_1$ and $\mathfrak{p}_2$ and there are no other inclusions between the prime ideals. So $\mathfrak{m}$ is an embedded ideal and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are isolated ideals.

Q2. Let K be a field. Show that the ideal $(x^2, xy, y^2) \subseteq K[x, y]$ is a primary ideal, which is not irreducible.

Solution. We first show that (x^2, xy, y^2) is primary. This simply follows from the fact that (x, y) is maximal ideal and from the fact that $(x^2, xy, y^2) = (x, y)^2$ (see after Lemma 6.4).

Now note that $(x^2, xy, y^2) = (x^2, y) \cap (x, y^2)$. Indeed, we clearly have $(x^2, xy, y^2) \subseteq (x^2, y) \cap (x, y^2)$. On the other hand, if $P(x, y) \in (x^2, y)$ then $P(x, y)$ has the form $P_1(x, y)x^2 + P_2(x, y)y$. Since $P_1(x, y)x^2$ is already in (x^2, xy, y^2), we thus only have to show that a polynomial of the form $P_2(x, y)y$, which lies in (x, y^2), necessarily lies in (x^2, xy, y^2). A polynomial in (x, y^2) is of the form $Q_1(x, y)y^2 + Q_2(x, y)x$. Now if we have $P_2(x, y)y = Q_1(x, y)y^2 + Q_2(x, y)x$ then $Q_2(x, y)$ is divisible by y and hence $Q_2(x, y)x = Q_2'(x, y)xy$ for some polynomial $Q_2'(x, y)$ so that $P_2(x, y)y \in (y^2, xy) \subseteq (x^2, xy, y^2)$, as required.

Q3. Let R be a noetherian ring and let T be a finitely generated R-algebra. Let G be a finite subgroup of the group of automorphisms of T as a R-algebra. Let T^G be the fixed point set of G (ie the subset of T, which is fixed by all the elements of G).

- Show that T is integral over T^G.

- Show that T^G is a subring of T, which contains the image of R and that T^G is finitely generated over R.

Solution. It is clear from the definitions that T^G is a subring which contains the image of R. Let $t \in T$. Then t satisfies the polynomial equation

$$\prod_{g \in G}(t - g(t)) = 0$$

The polynomial $M_t(x) := \prod_{g \in G}(x - g(t))$ has coefficients in T^G, because the coefficients are symmetric functions in the $g(t)$, which are invariant under G. Hence t is integral over T^G. Since t was arbitrary, T is integral over T^G. Since T is also finitely generated as a T^G-algebra (because it is finitely generated as a R-algebra), we thus see that T is finite over T^G (see after Lemma 6.6). Hence T^G is finitely generated over R by the Theorem of Artin-Tate.

Q4. Show that $\mathbb{Z}$ is integrally closed and that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

Solution. We first prove that $\mathbb{Z}$ is integrally closed. Let $p/q \in \mathbb{Q}$, where p and q are coprime integers, and let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be a monic polynomial. Suppose that $P(p/q) = 0$. Then we have

$$q^n P(p/q) = p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \cdots + a_0 q^n = 0.$$

Since $a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \cdots + a_0 q^n$ is divisible by q and p^n is coprime to q, this implies that $q = \pm 1$, so $p/q \in \mathbb{Z}$.

To prove that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$, note first that $\mathbb{Z}[i]$ is part of the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$. Indeed we have $(a + ib)^2 - 2a(a + ib) + a^2 + b^2 = 0$ for any $a, b \in \mathbb{Z}$. So we only have to prove that $\mathbb{Z}[i]$ is integrally closed in $\mathbb{Q}(i)$ (see Lemma 8.6). Note furthermore that $\mathbb{Q}(i)$ is the fraction field of $\mathbb{Z}[i]$. To see this, write let $r + it \in \mathbb{Q}(i)$, where $r, t \in \mathbb{Q}$ (any element of $\mathbb{Q}(i)$ can be written in this form because $\mathbb{Q}(i) \simeq \mathbb{Q}[x]/(x^2 + 1)$). Let $r = p/q$ and $t = u/v$. We then have $r + it = (vp + uqi)/(vq)$, which is a fraction of elements of $\mathbb{Z}[i]$, proving our claim. Finally, recall that we know from Rings and Modules that $\mathbb{Z}[i]$ is a Euclidean domain, where the Euclidean function is given by the norm (the norm of $c + id$ is $c^2 + d^2$ if $c + id \in \mathbb{Z}[i]$). In particular, $\mathbb{Z}[i]$ is a PID and every ideal in $\mathbb{Z}[i]$ is generated by an element of smallest norm.

To prove that $\mathbb{Z}[i]$ is integrally closed in $\mathbb{Q}(i)$, we may now proceed as for $\mathbb{Z}$. Let

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[i](x)$$

and let $r + it = B/A$, where $A, B \in \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, it is factorial and we may thus assume that $(A, B) = \mathbb{Z}[i]$. We can now write as before

$$A^n P(B/A) = B^n + a_{n-1}B^{n-1}A + a_{n-2}B^{n-2}A^2 + \cdots + a_0 A^n = 0.$$

Since $a_{n-1}B^{n-1}A + a_{n-2}B^{n-2}A^2 + \cdots + a_0A^n$ is divisible by A and B^n is coprime to A, this implies that A is a unit, so $B/A \in \mathbb{Z}[i]$.

Note that the proof above actually shows that any UFD (Unique Factorisation Domain) is integrally closed.

Q5. Let S be a ring and let $R \subseteq S$ be a subring of S. Suppose that R is integrally closed in S. Let $P(x) \in R[x]$ and suppose that $P(x) = Q(x)J(x)$, where $Q(x), J(x) \in S[x]$ and $Q(x)$ and $J(x)$ are monic. Show that $Q(x), J(x) \in R[x]$. Use this to give a new proof of the fact that if $T(x) \in \mathbb{Z}[x]$ and $T(x) = T_1(x)T_2(x)$, where $T_1(x), T_2(x) \in \mathbb{Q}[x]$ are monic polynomials, then $T_1(x), T_2(x) \in \mathbb{Z}[x]$.

Solution. We first prove the

Lemma. Let A be a ring and let $U(x) \in A[x]$ be a non zero monic polynomial. Then there exists a ring B containing A, which is integral over A and such that

$$U(x) = \prod_{i=1}^{\deg(U)} (x - b_i)$$

for some $b_i \in B$, where we set $\prod_{i=1}^{\deg(U)}(x - b_i) = 1$ if $\deg(U) = 0$.

Proof of the lemma. By induction on the degree $d = \deg(U)$ of $U(x)$. If $d = 0, 1$, there is nothing to prove. So suppose that $d > 1$ and that the result holds for any smaller value of d. The ring $C := A[y]/(P(y))$ is integral over A by Proposition 8.2. The element y of C satisfies the equation $P(y) = 0$ by construction. By Euclidean division (see Preamble), we thus have $P(x) = (x - y)Z(x)$ for some $Z(x) \in C[x]$. Since $Z(x)$ has degree $< d$, we may apply the inductive hypothesis and we obtain a ring B, which contains C and where $Z(x)$ splits. The polynomial $P(x)$ also splits in B, so we are done. □

We now apply the lemma to $Q(x)$ and $J(x)$ successively and we obtain a ring B, which contains S, such that B is integral over S and such that

$$Q(x) = \prod_{i=1}^{\deg(Q)} (x - b_i)$$

and

$$J(x) = \prod_{i=1}^{\deg(J)} (x - c_i)$$

where $b_i, c_i \in B$. Now we have $P(b_i) = P(c_i) = 0$ by construction, so the b_i and c_i are actually integral over R. Since the integral closure of R in B is a subring, we conclude that the coefficients of $Q(x)$ and $J(x)$ are integral over R (and in S, by assumption). But since R is integrally closed in S, this means that these coefficients lie in R.

Note that we did not actually use the fact that B was integral over S in the proof.

Q6. Let R be a subring of a ring T and suppose that T is integral over R. Let $\mathfrak{p}$ be prime ideal of R and let $\mathfrak{q}$ be a prime ideal of T. Suppose that $\mathfrak{q} \cap R = \mathfrak{p}$. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_k$ be primes ideal of R and suppose that $\mathfrak{p}_1 = \mathfrak{p}$. Show that there are prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_k$ of T such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all $i \in \{1, \ldots, k\}$.

Solution. By induction on k, we only need to treat the case $k = 2$. Consider the extension of rings $R/\mathfrak{p} \subseteq T/\mathfrak{q}$. This is also an integral extension. Furthermore, there is a unique prime ideal $\mathfrak{p}_2'$ in $R/\mathfrak{p}$, which corresponds to $\mathfrak{p}_2$ via the quotient map. By Theorem 8.8, there is a prime ideal $\mathfrak{q}_2'$ in $T/\mathfrak{q}$, which is such that $\mathfrak{q}_2' \cap R/\mathfrak{p} = \mathfrak{p}_2'$. The prime ideal $\mathfrak{q}_2$ corresponding to $\mathfrak{q}_2'$ via the quotient map has the required properties.

Q7. Let R be a ring. Let $\mathcal{S}$ be the set of ideals in R, which are not finitely generated.

(i) Let I be maximal element of $\mathcal{S}$ (with respect to the relation of inclusion). Show that I is prime.

(ii) Suppose that all the prime ideals of R are finitely generated. Prove that R is noetherian.

[Hint: exploit the fact that R/I is noetherian.]

Solution.

(i): Let $x, y \notin I$ and suppose for contradiction that $x, y \in I$. Let $I_x := (x) + I$ and $I_y = (y) + I$. Write $J := I_x \cdot I_y$. By assumption I_x, I_y and hence J are finitely generated, and we have $J \subseteq I$. Consider the image $I \pmod J$ of I in the R/I_y-module I_x/J. Note that I_x/J is finitely generated as a R/I_y-module since I_x is finitely generated as a R-module. Note also that the ring R/I_y is noetherian, since every ideal of R/I_y is the image of either the zero ideal or of an ideal of R strictly containing I. Hence $I \pmod J$ is also finitely generated as a R/I_y-module by Lemma 7.4. Let $m_1, \ldots, m_k$ be preimages in I of a finite set of generators of $I \pmod J$ as a R/I_y-module and let $y_1, \ldots, y_l$ be generators of J. Then $m_1, \ldots, m_k, y_1, \ldots, y_l$ is a finite set of generators of I, which is a contradiction.

(ii): If $\mathcal{T}$ is a totally ordered subset of $\mathcal{S}$ then the ideal $J := \cup_{H \in \mathcal{S}} H$ also lies in $\mathcal{S}$ (because if J were finitely generated then a finite set of generators of J would lie in one of the ideals in $\mathcal{T}$, and thus generate it, which is a contradiction). The ideal J is an upper bound for $\mathcal{T}$ and thus we may apply Zorn's lemma to conclude that there are maximal elements in $\mathcal{S}$, if $\mathcal{S}$ is not empty. By definition, $\mathcal{S}$ is empty iff R is noetherian. Hence, by (i), if R is not noetherian, there is a prime ideal, which is not finitely generated. The contraposition of this implication gives (i).

Q8. (optional). Let R be a ring. Let $\mathcal{S}$ be the set of non-principal ideals in R. Let I be a maximal element of $\mathcal{S}$. Prove that I is a prime ideal.

Solution.

Let $x, y \notin I$ and suppose for contradiction that $xy \in I$. Let $I_x := (x) + I$. By assumption, we have $I_x = (g_x)$ for some $g_x \in R$. Let $\phi : R \to I_x$ be the surjection of R-modules given by the formula $\phi(r) = rg_x$. We then have $I \subseteq \phi^{-1}(I)$.

Suppose first that $I = \phi^{-1}(I)$. In other words, for all $r \in R$, we have $rg_x \in I$ iff $r \in I$. This contradicts the fact that $yg_x \in I$. So we conclude that $I \subsetneq \phi^{-1}(I)$. From the definition of I, we then see that $\phi^{-1}(I)$ is a principal ideal of R, and hence so is $I = \phi(\phi^{-1}(I))$. This is a contradiction, so we cannot have $xy \in I$ if $x, y \notin I$. In other words, I is prime.