Exercise sheet 4. Prerequisites: all lectures. W1 of Trinity Term

Q1. Let R be a noetherian domain. Let $\mathfrak{m}$ be a maximal ideal in R. Let $r \in R\backslash\{0\}$ and suppose that (r) is a $\mathfrak{m}$-primary ideal. Show that $\mathrm{ht}((r)) = 1$.

Solution. By assumption, the nilradical of (r) is $\mathfrak{m}$. Since the nilradical is the intersection of all the prime ideals containing (r), we see that every prime ideal containing (r) also contains $\mathfrak{m}$. On the other hand, a prime ideal containing $\mathfrak{m}$ must be equal to $\mathfrak{m}$. We conclude that $\mathfrak{m}$ is the only prime ideal containing (r). In particular, $\mathfrak{m}$ is minimal among the prime ideals containing (r) and thus $\mathrm{ht}((r)) = \mathrm{ht}(\mathfrak{m}) \leq 1$ by Krull's principal ideal theorem. On the other hand, $\mathrm{ht}(\mathfrak{m}) = 1$, since we have the chain $\mathfrak{m} \supsetneq (0)$ (note that R is a domain).

Q2. Let A, B be integral domains and suppose that $A \subseteq B$. Suppose that A is integrally closed and that B is integral over A. Let

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

be a descending chain of prime ideals in A. Let $k \in \{0, \ldots, n-1\}$ and let

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_k$$

be a descending chain of prime ideals in B, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \in \{0, \ldots, k\}$. Then there is a descending chain of prime ideals

$$\mathfrak{q}_k \supsetneq \mathfrak{q}_{k+1} \supsetneq \cdots \supsetneq \mathfrak{q}_n$$

such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \in \{k+1, \ldots, n\}$. This is the "going-down theorem". See AT, Th. 5.16, p. 64. Let L (resp. K) be the fraction field of B (resp. A). Prove the going-down theorem when L is a (finite) Galois extension of K.

Solution. One immediately reduces the question to $n = 1$ and $k = 0$. Let $\bar{A}$ be the integral closure of A in L. Note that by assumption we have $B \subseteq \bar{A}$ and that $\bar{A}$ is integral over B (since it is integral over A). Let $\mathfrak{q}_0'$ be a prime ideal of $\bar{A}$ such that $\mathfrak{q}_0' \cap B = \mathfrak{q}_0$ (this exists by the (part of the) going-up theorem). Let $\mathfrak{a}$ be a prime ideal of $\bar{A}$ such that $\mathfrak{a} \cap A = \mathfrak{p}_1$ (again this exists by the going-up theorem). According to Q6 of sheet 2, there is a prime ideal $\mathfrak{b}$ in $\bar{A}$ such that $\mathfrak{b} \supsetneq \mathfrak{a}$ and such that $\mathfrak{b} \cap A = \mathfrak{p}_0$. According to Proposition 12.10, there is an element $\sigma \in \mathrm{Gal}(L|K)$ such that $\sigma(\mathfrak{b}) = \mathfrak{q}_0'$. We have $\sigma(\mathfrak{a}) \cap A = \mathfrak{p}_1$ and $\sigma(\mathfrak{a}) \subsetneq \sigma(\mathfrak{b}) = \mathfrak{q}_0'$. Hence $\sigma(\mathfrak{a}) \cap B \subseteq \mathfrak{q}_0' \cap B = \mathfrak{q}_0$ and $(\sigma(\mathfrak{a}) \cap B) \cap A = \sigma(\mathfrak{a}) \cap A = \mathfrak{p}_1$. Furthermore, we have $\sigma(\mathfrak{a}) \cap B \subsetneq \mathfrak{q}_0$ because $\sigma(\mathfrak{a}) \cap A = \mathfrak{p}_1 \subsetneq \mathfrak{q}_0 \cap A = \mathfrak{p}_0$. So we may set $\mathfrak{q}_1 := \sigma(\mathfrak{a}) \cap B$.

Q3. Let R be an integrally closed domain. Let $K := \mathrm{Frac}(R)$. Let $L|K$ be an algebraic field extension. Show that an element $e \in L$ is integral over R iff the minimal polynomial of e over K has coefficients in R.

Solution. Let $P(x) \in K[x]$ be the minimal polynomial of e. If $P(x) \in R[x]$ then e is integral over R by the definition of integrality. On other hand, suppose that e is integral over R and let $Q(x) \in R[x]$ be a monic polynomial such that $Q(e) = 0$. Then $P(x)$ divides $Q(x)$ by the definition of the minimal polynomial and $P(x) \in R[x]$ by Q5 of sheet 2.

Q4. Let R be a PID. Suppose that $2 = 1 + 1$ is a unit in R. Let $c_1, \ldots, c_t \in R$ be distinct irreducible elements and let $c := c_1 \cdots c_t$. Show that the ring $R[x]/(x^2 - c)$ is a Dedekind domain. Use this to show that $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ is a Dedekind domain.

Solution. Let $K := \mathrm{Frac}(R)$. Notice first that c is not a square in K.

Indeed, suppose for contradiction that there is an element $e \in K$ such that $e^2 = c$. Write $e = f/g$, with

$f, g \in R$ and f and g coprime. We then have $f^2/g^2 = c$ and hence $f^2 = g^2 c$. In particular, c_1 divides f and thus c_1^2 divides $g^2 c$. Since $(f, g) = 1$, we deduce that c_1^2 divides c, which contradicts our assumptions.

We deduce that the polynomial $x^2 - c$ is irreducible over K, since it has no roots in K. Let $L := K[y]/(y^2 - c)$. Note that L is a field, since $y^2 - c$ is irreducible. Now let $\phi : R[x] \to L$ be the homomorphism of R-algebras, which sends x to $y \,(\mathrm{mod}\,(y^2 - c))$. We have $\phi(Q(x)) = Q(y) = 0$ iff $x^2 - c$ divides $Q(x)$ in $K[x]$. On the other hand, if $x^2 - c$ divides $Q(x)$ in $K[x]$, then $x^2 - c$ divides $Q(x)$ in $R[x]$ by the unicity statement in the Euclidean algorithm (see preamble). Hence $\ker(\phi) = (x^2 - c)$. We thus see that $R[x]/(x^2 - c)$ can be identified with the sub-R-algebra of L generated by y. Under this identification, the elements of $R[x]/(x^2 - c)$ correspond to the elements of the form $\lambda + \mu y$, with $\lambda, \mu \in R$, whereas the elements of K can all be written as $\lambda + \mu y$, with $\lambda, \mu \in K$.

We claim that that L is the fraction field of $R[x]/(x^2 - c)$. Note first that the fraction field of $R[x]/(x^2 - c)$ naturally embeds in L, since L is field containing $R[x]/(x^2 - c)$. To prove the claim, we only have to show that every element of L can be written as a fraction in L of elements of $R[x]/(x^2 - c)$. This simply follows from the fact that if $f, g, h, j \in R$ and $f/g + (h/j)y \in L$, then

$$f/g + (h/j)y = \frac{fj + hgy}{gj}.$$

Now to prove that $R[x]/(x^2 - c)$ is a Dedekind domain, we have to show that it is noetherian, that is has dimension 1 and that it is integrally closed. The ring $R[x]/(x^2 - c)$ is clearly noetherian (by the Hilbert basis theorem and Lemma 7.2). Also, the ring $R[x]/(x^2 - c)$ is integral over R by construction and R has dimension one by Lemma 11.19. We deduce from Lemma 11.29 that $R[x]/(x^2 - c)$ also has dimension 1. To show that $R[x]/(x^2 - c)$ is integrally closed, we have to show that the integral closure of $R[x]/(x^2 - c)$ in L is $R[x]/(x^2 - c)$. The integral closure of $R[x]/(x^2 - c)$ in L is also the integral closure of R in L by Lemma 8.6 (since $R[x]/(x^2 - c)$ consists of elements, which are integral over R). Furthermore, by Q3 an element $\lambda + \mu y \in L$ is integral iff its minimal polynomial $P(t) \in K[t]$ has coefficients in R. Thus we have to show that if $\lambda + \mu y \in L$ has a minimal polynomial $P(t) \in R[t]$ then $\lambda, \mu \in R$. We prove this statement.

If $\mu = 0$ then $\lambda + \mu y \in R$ and thus the minimal polynomial of $\lambda + \mu y$ is $t - \lambda$. So the statement certainly holds in this situation.

If $\mu \neq 0$, we note that the polynomial

$$(t - (\lambda + \mu y))(t - (\lambda - \mu y)) = t^2 - 2\lambda + \lambda^2 - \mu^2 y^2 = t^2 - 2\lambda + \lambda^2 - c\mu^2$$

annihilates $\lambda + \mu y$ and has coefficients in K. It must thus coincide with the minimal polynomial $P(t)$ of $\lambda + \mu y$, since we know that $\deg(P(t)) > 1$.

Thus we have to show that if $-2\lambda \in R$ and $\lambda^2 - c\mu^2 \in R$, then $\lambda, \mu \in R$. So suppose that $-2\lambda \in R$ and $\lambda^2 - c\mu^2 \in R$. We have $\lambda \in R$, since -2 is a unit in R by assumption. Hence $c\mu^2 \in R$. We claim that $\mu \in R$. Indeed, let $\mu = f/g$, where $f, g \in R$ and f and g are coprime. Then $cf^2 = g^2 r$ for some $r \in R$. Let $i \in \{1, \dots, t\}$ and suppose first that c_i divides g. Then c_i^2 divides rg^2 and since c_i appears with multiplicity one in c by assumption, we thus see that c_i divides f, which is a contradiction (because $(f, g) = 1$). Hence c_i does not divide g and thus c_i divides r. Since all the c_i are distinct, we thus see that c divides r and thus $(f/g)^2 = r/c =: d \in R$. Hence $f^2 = g^2 d$. Since f and g are coprime, we see that f^2 divides d and hence $d/f^2 \in R$. Since $g^2(d/f^2) = 1$, we conclude that g is a unit and hence $\mu = f/g \in R$.

To see that $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ is a Dedekind domain, note that $\mathbb{R}[x, y]/(x^2 + y^2 - 1) \simeq (\mathbb{R}[x])[y]/(y^2 - (1 - x^2))$ and apply the first statement of the question with $R = \mathbb{R}[x]$ and $c = 1 - x^2 = (1 - x)(1 + x)$.

Q5. Let R be a PID. Suppose that $2 = 1+1$ is invertible in R. Let $c_1, c_2 \in R$ be two distinct irreducible elements and let $c := c_1 \cdot c_2$. Show that the decomposition of the ideal (c) in $R[x]/(x^2-c)$ into a product of prime ideals is $(c) = (x, c_1)^2 \cdot (x, c_2)^2$ (noting that $R[x]/(x^2-c)$ is a Dedekind domain by Q4).

Solution. Note first that (x, c_i) $(i = 1, 2)$ is indeed a prime ideal of $R[x]/(x^2-c)$, because

$$(R[x]/(x^2-c))/(x, c_i) = R[x]/(x^2-c, x, c_i) = R/(-c, c_i) = R/(c_i),$$

which is a domain, since c_i is irreducible.

We only have to show that $(c_i) = (x, c_i)^2$.

We first show that $(c_i) \subseteq (x, c_i)^2$. For this, note that $c_i^2 \in (x, c_i)^2$ by definition and

$$(x - c_i)(x + c_i) = x^2 - c_i^2 = c - c_i^2 = c_i(c_j - c_i) \in (x, c_i)^2,$$

where $j = 1$ if $i = 2$ and $j = 2$ if $i = 1$. But $\gcd_R(c_i^2, c_i(c_j - c_i)) = c_i$ (because $c_j - c_i$ is coprime to c_i in R, since c_j is irreducible and distinct from c_i), and in particular $c_i \in (x, c_i)^2$, so that $(c_i) \subseteq (x, c_i)^2$.

To show that $(c_i) \supseteq (x, c_i)^2$, we only have to show that $(x, c_i)^2 \,(\mathrm{mod}\,(c_i)) = ((x, c_i)\,(\mathrm{mod}\,(c_i)))^2 = 0$ in $(R[x]/(x^2-c))/(c_i)$. Now we have $(R[x]/(x^2-c))/(c_i) = R[x]/(x^2-c, c_i) = (R/(c_i))[x]/x^2$. The image $(x, c_i)\,(\mathrm{mod}\,(c_i))$ of (x, c_i) in $(R/(c_i))[x]/x^2$ is generated by x, so that $((x, c_i)\,(\mathrm{mod}\,(c_i)))^2 = 0$.

Q6. Let R be a ring (not necessarily noetherian). Suppose that $\dim(R) < \infty$.

Show that $\dim(R[x]) \leq 1 + 2\dim(R)$.

Solution. Let

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \mathfrak{q}_2 \supsetneq \cdots \supsetneq \mathfrak{q}_d$$

be a descending chain of prime ideals in $R[x]$, where $d \geq 0$. By restriction, we obtain a descending chain of prime ideals

$$\mathfrak{q}_0 \cap R \supseteq \mathfrak{q}_1 \cap R \supseteq \mathfrak{q}_2 \cap R \supseteq \cdots \supseteq \mathfrak{q}_d \cap R \quad (*)$$

(possibly with repetitions) in R. For each $i \in \{0, \ldots, d\}$, let $\rho(i) \geq 0$ be the largest integer k such that $\mathfrak{q}_i \cap R = \mathfrak{q}_{i+1} \cap R = \cdots = \mathfrak{q}_{i+k} \cap R$. By Lemma 11.21 (and the remark before it) and Lemma 11.19 we have $\rho(i) \leq 1$ for all $i \in \{0, \ldots, d\}$. Now let

$$\mathfrak{q}_{i_0} \cap R = \mathfrak{q}_0 \cap R \supsetneq \mathfrak{q}_{i_1} \cap R \supsetneq \cdots \supsetneq \mathfrak{q}_{i_\delta} \cap R$$

be an enumeration of all the prime ideals appearing in the chain $(*)$, in decreasing order of inclusion. We have

$$d + 1 = (1 + \rho(i_0)) + (1 + \rho(i_1)) + \cdots + (1 + \rho(i_\delta)) \leq 2(\delta + 1)$$

so that $d \leq 2\delta + 1$. Now we have $\delta \leq \dim(R)$ and the required inequality follows.

Q7. Let R be a Dedekind domain. Let $\mathfrak{a}$ be a non zero ideal in R. Show that every ideal in $R/\mathfrak{a}$ is principal. Show that every ideal in a Dedekind domain can be generated by two elements.

Solution. We first prove the first statement. Since R is a Dedekind domain, we have a primary decomposition

$$\mathfrak{a} = \bigcap_{i=1}^{k} \mathfrak{p}_i^{m_i}$$

for some prime ideals $\mathfrak{p}_i$. Using Lemma 12.2 and the Chinese remainder theorem, we see that we have

$$R/\mathfrak{a} \simeq \bigoplus_{i=1}^{k} R/\mathfrak{p}_i^{m_i}$$

Now an ideal I of $\bigoplus_{i=1}^{k} R/\mathfrak{p}_i^{m_i}$ is of the form $\bigoplus_{i=1}^{k} I_i$, where I_i is an ideal of $R/\mathfrak{p}_i^{m_i}$. This follows from the fact that if $e \in I$ and $e = \oplus_{i=1}^{k} e_i$ then $e_i = e \cdot (0, \ldots, 1, \ldots, 0) \in I$, where 1 appears in the i-th place in the expression $(0, \ldots, 1, \ldots, 0)$. Hence, if we can find generators $g_i \in I_i$ for I_i in $R/\mathfrak{p}_i^{m_i}$, then $(g_1, \ldots, g_k)$ will be a generator of I. We proceed to show that any ideal in $R/\mathfrak{p}_i^{m_i}$ can be generated by one element. Consider the exact sequence

$$0 \to \mathfrak{p}_i^{m_i} \to R \to R/\mathfrak{p}_i^{m_i} \to 0$$

Localising this sequence at $R \backslash \mathfrak{p}_i$, we get the sequence of $R_\mathfrak{p}$-modules

$$0 \to (\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i} \to R_{\mathfrak{p}_i} \to (R/\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i} \to 0$$

Now the $R_\mathfrak{p}$-submodule $(\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i}$ of $R_\mathfrak{p}$ is the ideal generated by the image of $\mathfrak{p}_i^{m_i}$ in $R_\mathfrak{p}$ (see the beginning of the proof of Lemma 5.6). If we let $\mathfrak{m}$ be the maximal ideal of $R_\mathfrak{p}$, this is also $\mathfrak{m}^{m_i}$. On the other hand, $\mathfrak{p}_i$ is contained in the nilradical of $\mathfrak{p}_i^{m_i}$ and since $\mathfrak{p}_i$ is maximal (by Lemma 12.1) it coincides with the radical of $\mathfrak{p}_i^{m_i}$. Hence $R/\mathfrak{p}_i^{m_i}$ has only one maximal ideal, namely $\mathfrak{p}_i \,(\mathrm{mod}\, \mathfrak{p}_i^{m_i})$. Since the image of $R \backslash \mathfrak{p}_i$ in $R/\mathfrak{p}_i^{m_i}$ lies outside $\mathfrak{p}_i \,(\mathrm{mod}\, \mathfrak{p}_i^{m_i})$, we see that this image consists of units. Hence $(R/\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i} \simeq R/\mathfrak{p}_i^{m_i}$. All in all, there is thus an isomorphism

$$R_{\mathfrak{p}_i}/\mathfrak{m}^{m_i} \simeq R/\mathfrak{p}_i^{m_i}.$$

Now by Proposition 12.4, every ideal in $R_{\mathfrak{p}_i}/\mathfrak{m}^{m_i}$ is principal, and so we have proven the first statement.

For the second one, let $e \in \mathfrak{a}$ be any non-zero element. Then the ideal $\mathfrak{a} \,(\mathrm{mod}\, (e)) \subseteq R/(e)$ is generated by one element, say g. Let $g' \in R$ be a preimage of g. Then $\mathfrak{a} = (e, g')$.

Q8. (optional) Let A (resp. B) be a noetherian local ring with maximal ideal $\mathfrak{m}_A$ (resp. $\mathfrak{m}_B$). Let $\phi : A \to B$ be a ring homomorphism and suppose that $\phi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$ (such a homomorphism is said to be 'local').

Suppose that

(1) B is finite over A via ϕ;

(2) the map $\mathfrak{m}_A \to \mathfrak{m}_B/\mathfrak{m}_B^2$ induced by ϕ is surjective;

(3) the map $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ induced by ϕ is bijective.

Prove that ϕ is surjective. [Hint: use Nakayama's lemma twice].

Solution. By Corollary 3.6, the image of of $\mathfrak{m}_A$ in $\mathfrak{m}_B$ generates $\mathfrak{m}_B$ as a B-module. In other words, $\phi(\mathfrak{m}_A)B = \mathfrak{m}_B$. On the other hand, since B is finitely generated as a A-module, the homomorphism ϕ is surjective iff the induced map $A/\mathfrak{m}_A \to B/\phi(\mathfrak{m}_A)B$ is surjective, again by Corollary 3.6. Now $B/\phi(\mathfrak{m}_A)B = B/\mathfrak{m}_B$ by the above and by (3) the map $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ is surjective. The conclusion follows.

Q9. (optional) Let R be a Dedekind domain. Show that R is a PID iff it is a UFD.

Solution. See https://planetmath.org/pidandufdareequivalentinadedekinddomain