B2.2 Commutative Algebra

Sheet 5 — HT26

Section 11 (for the interested readers)

Section C

1. 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

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

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

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

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

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

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 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 $\mathfrak{b} \supset \mathfrak{a}$ 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 $\sigma(\mathfrak{a}) \subset \sigma(\mathfrak{b}) = \mathfrak{q}'_0$. Hence $\sigma(\mathfrak{a}) \cap B \subseteq \mathfrak{q}'_0 \cap B = \mathfrak{q}_0$ and $(\sigma(\mathfrak{a}) \cap B) \cap A = \sigma(\mathfrak{a}) \cap A = \mathfrak{p}_1$. So we may set $\mathfrak{q}_1 = \sigma(\mathfrak{a}) \cap B$.

2. Let R be a Dedekind domain. Let I be a non zero ideal in R. Show that every ideal in R/I is principal. Deduce that every ideal in a Dedekind domain can be generated by two elements.

Dawid Kielak: kielak@maths.ox.ac.uk

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

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

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

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

Now an ideal J of $\bigoplus_{i=1}^{k} R/\mathfrak{p}_i^{m_i}$ is of the form $\bigoplus_{i=1}^{k} J_i$, where J_i is an ideal of $R/\mathfrak{p}_i^{m_i}$. This follows from the fact that if $e \in J$ and $e = \oplus_{i=1}^{k} e_i$ then $e_i = e \cdot (0, \dots, 1, \dots, 0) \in J$, where 1 appears in the i-th place in the expression $(0, \dots, 1, \dots, 0)$. Hence, if we can find generators $g_i \in J_i$ for J_i in $R/\mathfrak{p}_i^{m_i}$, then $(g_1, \dots, g_k)$ will be a generator of J. 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 $R \setminus \mathfrak{p}_i$, we get the exact sequence of $R_{\mathfrak{p}_i}$-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 $R_{\mathfrak{p}_i}$-submodule $(\mathfrak{p}_i^{m_i})_{\mathfrak{p}_i}$ of $R_{\mathfrak{p}_i}$ is the ideal generated by the image of $\mathfrak{p}_i^{m_i}$ in $R_{\mathfrak{p}_i}$ (see the beginning of the proof of Lemma 5.6). If we let $\mathfrak{m}$ be the maximal ideal of $R_{\mathfrak{p}_i}$, this is also $\mathfrak{m}^{m_i}$. On the other hand, $\mathfrak{p}_i$ is contained in the nilradical of $R/\mathfrak{p}_i^{m_i}$ and since $\mathfrak{p}_i$ is maximal (by Lemma 12.1) it coincides with the radical of $R/\mathfrak{p}_i^{m_i}$. Hence $R/\mathfrak{p}_i^{m_i}$ has only one maximal ideal, namely $\mathfrak{p}_i$ mod $\mathfrak{p}_i^{m_i}$. Since the image of $R \setminus \mathfrak{p}_i$ in $R/\mathfrak{p}_i^{m_i}$ lies outside $\mathfrak{p}_i$ 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 $e \in I$ be any non-zero element. Then the ideal I mod $(e) \subseteq R/(e)$ is generated by one element, say g. Let $g' \in R$ be a preimage of g. Then $I = (e, g')$.

Dawid Kielak: kielak@maths.ox.ac.uk

3. 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 with $t \geqslant 1$, 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 $f^2 = g^2c$. In particular, c_1 divides f and thus c_1^2 divides g^2c. 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 $L = K[x]/(x^2 - c)$. Note that L is a field, since $x^2 - c$ is irreducible. Now let $\phi\colon R[x] \to L$ be the obvious homomorphism of R-algebras. We have $\phi(Q(x)) = 0$ if and only if $x^2 - c$ 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 x. Under this identification, the elements of $R[x]/(x^2 - c)$ correspond to the elements of the form $\lambda + \mu x$, with $\lambda, \mu \in R$, whereas the elements of L can all be written as $\lambda + \mu x$, 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 a 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 $f/g + (h/j)x \in L$, then

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

   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.

   Since R contains an irreducible element c_1, it cannot be a field.

   The ring $R[x]/(x^2 - c)$ is clearly noetherian (by the Hilbert basis theorem and stability of noetherianity under quotients). Also, the ring $R[x]/(x^2 - c)$ is integral over R since every element of $R[x]/(x^2 - c)$ squared can be expressed as a linear polynomial in $R[x]/(x^2 - c)$ with coefficients in R. Also, R has dimension one by Question 2. 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, since $R[x]/(x^2 - c)$ consists of elements that are integral

Dawid Kielak: kielak@maths.ox.ac.uk

over R. Furthermore, by Question 4, an element $\lambda + \mu x \in L$ is integral over R if and only if its minimal polynomial $P(t) \in K[t]$ has coefficients in R. Thus we have to show that if $\lambda + \mu x \in L$ has a minimal polynomial $P(t) \in R[t]$ then $\lambda, \mu \in R$. We prove this statement.

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

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

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

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 $c = 1 - x^2 = (1-x)(1+x)$.

4. Let R be a Dedekind domain. Show that R is a PID if and only if it is a UFD.

Solution: Every PID is a UFD.

For the converse, first note that it is enough to prove that all prime ideals are principal, since every non-trivial proper ideal in a Dedekind domain is a product of prime ideals.

Let $\mathfrak{p}$ be a non-trivial prime ideal in R. Since R is a UFD, there is a prime element $p \in \mathfrak{p}$. Hence we have the inclusions

$$(0) \subset (p) \subseteq \mathfrak{p},$$

and since $\dim R = 1$ we must have $\mathfrak{p} = (p)$.

Dawid Kielak: kielak@maths.ox.ac.uk