January 27, 2018

Number Theory I (Commutative Algebra)

Hélène Esnault, Exercises: Shane Kelly

Exercise sheet 12

As in the textbook, all rings are commutative with a unit.

The reference [Jud] is to Judson, "Abstract algebra, theory and applications", August 5, 2017.

The goal of this exercise sheet is to show that if k is a field, then $k[x_1, \dots, x_n]$ is a unique factorisation domain (UFD).

We will admit as given that: if K is any field, then $K[x]$ is a principal ideal domain (PID) [Jud, 17.6, 17.20], and therefore a UFD [Jud, 18.15].

Let D be a domain. Recall that a polynomial in $D[y]$ is *primitive* if no non-invertible element of D divides all its coefficients at once.

Exercise 1 ([Jud, 18.26, 18.27])**.** Let D be a UFD and $K = \mathrm{Frac}(D)$. Let $p(y) \in D[y]$ and $p(y) = f(y)g(y)$ where $f(y), g(y) \in K[y]$. Show that:

(1) There exists $a, b \in D$ such that af and bg are in $D[y]$.
(2) There exists $a_1, b_1 \in D$, and primitive polynomials $f_1(y), g_1(y) \in D[y]$ such that $af = a_1 f_1$ and $bg = b_1 g_1$, with $\deg f = \deg f_1$ and $\deg g = \deg g_1$.
(3) There exists $c \in D$, and primitive polynomials $f_1(y), g_1(y) \in D[y]$ such that $p(y) = cf_1(y)g_1(y)$, with $\deg f = \deg f_1$ and $\deg g = \deg g_1$.
(4) Assume that $p(y) \in D[y]$ is primitive. Show that $p(y)$ is irreducible in $D[y]$ if and only if it is irreducible in $K[y]$.

Exercise 2 ([Jud, 18.29])**.** Suppose that D is a UFD (e.g., $D = \mathbb{Z}$ or $D = \mathbb{C}[x]$). In this exercise we show that $D[y]$ is also a UFD.

(1) Let $K = \mathrm{Frac}(D)$. Using the embedding $D[y] \subset K[y]$, show that every element $p(y) \in D[y]$ can be written as:
  (a) A product $p(y) = f_1(y) \dots f_n(y)$ with each $f_i(y) \in K[y]$ irreducible in $K[y]$.
  (b) A product $p(y) = \frac{1}{a_1 \dots a_n} g_1(y) \dots g_n(y)$ with $a_i \in D$ and $g_i(y) \in D[y]$ such that each $g_i(y)$ is irreducible in $K[y]$.
  (c) A product $p(y) = \frac{b_1 \dots b_n}{a_1 \dots a_n} h_1(y) \dots h_n(y)$ with $b_i \in D$ and $h_i(y) \in D[y]$ such that each $h_i(y)$ is primitive in $D[y]$ and irreducible in $K[y]$.
  (d) A product $p(y) = ch_1(y) \dots h_n(y)$ with $c \in D$ and $h_i(y) \in D[y]$ such that each $h_i(y)$ is primitive in $D[y]$ and irreducible in $K[y]$.
  (e) A product $p(y) = uc_1 \dots c_m h_1(y) \dots h_n(y)$ with $u \in D^*$ a unit, $c_i \in D$ irreducible in D, and $h_i(y) \in D[y]$ irreducible in $D[y]$ (cf. Exercise 2(4) above).

  Deduce that every element of $D[y]$ can be written (possibly non-uniquely) as a product of irreducible elements.
(2) Suppose $a_1 \dots a_m f_1(y) \dots f_n(y) = b_1 \dots b_r g_1(y) \dots g_s(y)$ where $a_i, b_i \in D$ are irreducible, and $f_i, g_i \in D[x]$ are also irreducible.
  (a) By considering the embedding $D[y] \subset K[y]$, show that $s = n$, and that, up to relabelling, $\frac{c_i}{d_i} f_i = g_i$ for some $c_i, d_i \in D$.
  (b) Notice that since the f_i, g_i are irreducible in $D[x]$, they are primitive. Deduce from this that the c_i, d_i from the previous step satisfy $u_i c_i = d_i$

for some unit $u_i \in D^*$. In other words,

$$u_i f_i = g_i.$$

(c) Since $D[y]$ is a domain deduce that $ua_1 \dots a_m = b_1 \dots b_r$ for some $u \in D^*$.

(d) Since D is a UFD, deduce that $m = s$ and, up to relabelling,

$$v_i a_i = b_i$$

for some $v_i \in D^*$.

Deduce that the factorisation from part (1) is unique, up to relabelling and multiplication by units.

(3) Deduce that $D[y]$ is a UFD.

Exercise 3 ([Jud, 18.32])**.** Show that if k is a field, then the ring of polynomials $k[x_1, \dots, x_n]$ is a UFD.