Solution 6

Unique Factorization Domains

1. Let R be a UFD. Let that $a, b \in R$ be coprime elements (that is, $\gcd(a,b) \in R^\times$) and $c \in R$. Suppose that $a|c$ and $b|c$. Prove that $ab|c$.

   Solution: By assumption, there exist $r, s \in R$ such that $ar = c = bs$. In order to prove the statement, it is enough to show that $a|s$. Since R is a UFD, there exist $u, v, w, z \in R^\times$, $n_a, n_b, n_s, n_r \in \mathbb{Z}_{\geqslant 0}$ and irreducible elements $a_1, \ldots, a_{n_a}$, $r_1, \ldots, r_{n_r}$, $b_1, \ldots, b_{n_b}$ and $s_1, \ldots, s_{n_s} \in R$ such that

   $$a = ua_1 \cdots a_{n_a},\ r = vr_1 \cdots r_{n_r},\ b = wb_1 \cdots b_{n_b},\ s = zs_1 \cdots s_{n_s}.$$

   Then $ar = bs$ reads

   $$a_1 \cdots a_{n_a}(uvr_1)r_2 \cdots r_{n_r} = b_1 \cdots b_{n_b}(wzs_1)s_2 \cdots s_{n_s} \tag{1}$$

   and by uniqueness of factorization each a_i is associated to some b_i or some s_i. Suppose that, for some i, a_i is associated to b_j. Then $a_i | \gcd(a,b) \in R^\times$, a contradiction. Hence each a_i divides one of the elements s_j, and since in the decomposition (1) the associated elements on the two sides can be taken in a bijective correspondence, we can choose for each i a distinct j_i such that $s_{j_i} = \lambda_i a_i$, so that

   $$\lambda_1 \cdots \lambda_{n_a} a = \lambda_1 \cdots \lambda_{n_a} a_1 \cdots a_{n_a} = s_{j_1} \cdots s_{j_{n_a}} | s,$$

   so that $a|s$ and $ab|c$ as desired.

2. We use the notation $\sqrt{-5} = i\sqrt{5} \in \mathbb{C}$. Let $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Consider the map $N : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}$ sending $x = a + b\sqrt{-5} \mapsto a^2 + 5b^2 = x\overline{x}$.

   (a) Prove that N is a multiplicative map with image inside $\mathbb{N}$.

   (b) Show that $\mathbb{Z}[\sqrt{-5}]^\times = \{x \in \mathbb{Z}[\sqrt{-5}] : N(x) = 1\} = \{\pm 1\}$.

   (c) Prove that the elements 2 and $1 + \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$ and that they are coprime in the sense that the only common divisors of those are units. [*Hint:* If $x|y$, then $N(x)|N(y)$]

   (d) Using Exercise 1, deduce that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD [*Hint:* $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$]

   (e) Is $2 \in \mathbb{Z}[\sqrt{-5}]$ a prime element?

   Solution:

(a) For each $x, y \in \mathbb{Z}[\sqrt{-5}]$, we see that $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$, meaning that N is a multiplicative map. As $N(a + \sqrt{-5}b) = a^2 + 5b^2$ and $a^2, 5b^2$ are non-negative integers for all $a, b \in \mathbb{Z}$, the norm has image inside $\mathbb{N}$.

(b) Let $x \in \mathbb{Z}[\sqrt{-5}]^\times$ and write $xy = 1$ for some $y \in \mathbb{Z}[\sqrt{-5}]$. Then $N(x)N(y) = N(xy) = N(1) = 1^2 + 0 = 1$, so that $N(1)|1$ and since $N(1) \in \mathbb{N}$ by part (a), we conclude that $N(x) = 1$. Hence there is an inclusion of sets $\mathbb{Z}[\sqrt{-5}]^\times \subseteq \{x \in \mathbb{Z}[\sqrt{-5}] : N(x) = 1\}$. Now suppose that $N(x) = 1$ for $x = a + \sqrt{-5}b$, i.e., $a^2 + 5b^2 = 1$. Then $b = 0$ (because else $N(x) \geqslant 5$) from which it follows $a^2 = 1$ and the unique possibilities are $x = \pm 1$. Hence $\{x \in \mathbb{Z}[\sqrt{-5}] : N(x) = 1\} \subseteq \{\pm 1\}$. Finally, the elements ± 1 are clearly units, so that $\{\pm 1\} \subseteq \mathbb{Z}[\sqrt{-5}]^\times$. This allows us to conclude that the three sets are equal.

(c) Suppose that $2 = xy$ for some $x, y \in \mathbb{Z}[\sqrt{-5}]$. Then

$$4 = N(2) = N(xy) = N(x)N(y)$$

so that $N(x) \in \{1, 2, 4\}$. Writing $x = a + \sqrt{-5}b$, we see that the equality $a^2 + 5b^2 = 2$ cannot hold (because b must vanish, but then $a^2 = 2$ is a contradiction with $a \in \mathbb{Z}$), so that $N(x) = 1$, in which case x is a unit, or $N(x) = 4$, in which case $N(y) = 1$ and y is a unit. Hence 2 is irreducible. Similarly, $N(1 + \sqrt{-5}) = 6$ tells us that a proper divisor of $1 + \sqrt{-5}$ could only have norm 2 or 3, which are both impossible situations (as the equality $a^2 + 5b^2 = 3$ cannot hold for $a, b \in \mathbb{Z}$, too), so that $1 + \sqrt{-5}$ is irreducible. Suppose by contradiction that 2 and $1+\sqrt{-5}$ have a common divisor $p \notin R^\times$. As they are both irreducible, the only possibility is that p is associated to both 2 and $1 + \sqrt{-5}$ so that 2 and $1 + \sqrt{-5}$ are associated, a contradiction (because $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$, but clearly $2 \neq \pm(1 + \sqrt{-5})$). Hence 2 and $1 + \sqrt{-5}$ are not coprime.

(d) Suppose by contradiction that $\mathbb{Z}[\sqrt{-5}]$ is a UFD. Then 2 and $1 + \sqrt{-5}$ are coprime in the sense that $\gcd(2, 1 + \sqrt{-5}) \in R^\times$. Moreover, they both divide $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ so that $2(1 + \sqrt{-5})|6$ by Exercise 1. But

$$N(2(1 + \sqrt{-5})) = 24 \nmid 36 = N(6),$$

a contradiction. Hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

(e) The element 2 is not prime, because it divides $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but it does not divide $1 + \sqrt{-5}$ since $N(2) = 4 \nmid 6 = N(1 + \sqrt{-5})$.

3. Let K be a field and $f \in K[X]$.

(a) Let $x_1, \ldots, x_n \in K$ be distinct roots of f. Prove that

$$\prod_{i=1}^{n}(X - x_i)|f.$$

(b) Let $d = \deg(f)$ and $x_1, \ldots, x_d \in K$ be distinct roots of f. Prove that there exists $c \in K^\times$ such that

$$f = c \prod_{i=1}^{d} (X - x_i).$$

Solution:

(a) As seen in class and in previous assignments, if $x \in K$ is a root of f, then $X - x | f$. By assumption, $X - x_1, \ldots, X - x_n | f$. The elements $X - x_i$ are pairwise coprime in $K[X]$, so that for each k the elements $\prod_{i=1}^{k-1}(X - x_i)$ and $X - x_k$ are coprime in $K[X]$ and since $K[X]$ is a UFD, we obtain by induction that $\prod_{i=1}^{n}(X - x_i) | f$ by Exercise 1.

Alternative solution: The statement actually works also when K is just an integral domain. We can indeed prove that $\prod_{i=1}^{n}(X - x_i) | f$ by induction on n. The case $n = 1$ is clear by assumption. Now suppose that the statement is proven for $n - 1$ and let $x_1, \ldots, x_n \in K$ be distinct roots of f. Then $\prod_{i=1}^{n-1}(X - x_i) | f$ by inductive hypothesis so that we can write

$$f = g \prod_{i=1}^{n-1} (X - x_i).$$

Since $0 = f(x_n) = g(x_n) \prod_{i=1}^{n-1}(x_n - x_i)$ and all the terms $x_n - x_i$ are non-zero, the fact that K is an integral domain implies that $g(x_n) = 0$, so that $X - x_n | g$ and we are done.

(b) By part (a), there exists $g \in K[X]$ such that

$$f = g \prod_{i=1}^{d} (X - x_i)$$

and by looking at the degrees we see that

$$d = \deg(f) = \deg(g) + \sum_{i=1}^{d} \deg(X - x_i) = \deg(g) + d$$

so that $\deg(g) = 0$ and $g \in K^\times$.

4. Let K be a field. Prove that X and Y are coprime elements in $K[X, Y]$, but that the ideals (X) and (Y) are not coprime. [Recall that two ideals I, J of R are called coprime if $I + J = R$]

Solution: Let $f \in K[X, Y]$ and suppose that $f | X, Y$. Clearly $f \neq 0$. Moreover, $\deg_Y(f) \leqslant \deg_Y(X) = 0$ and $\deg_X(f) \leqslant \deg_X(Y) = 0$, so that f is constant. Hence $f \in K \setminus \{0\} = K^\times$. This implies that X and Y are coprime. On the other hand, the ideal (X, Y) is proper, because its elements have all trivial evaluation at $(0, 0)$, whereas $1 \in K[X, Y]$ does not.

5. Let R be a UFD with $K = \mathrm{Frac}(R)$. Let $f \in R[X]$ be a non-constant polynomial. Prove that f is irreducible in $R[X]$ if and only if it is primitive and irreducible in $K[X]$.

   Solution: Recall that $R[X]^\times = R^\times$ and $K[X]^\times = K^\times$, since R and K are integral domains. As f is assumed to be non-constant, it cannot be a unit neither trivial, so that the statement that saying that f is not irreducible is equivalent to saying that f is reducible, i.e., that it is the product of two not invertible elements. We prove the statement by contraposition, that is, we prove that f has a non-trivial decomposition in $R[X]$ if and only if it is not primitive or it has a non-trivial decomposition in $K[X]$.

   Suppose that f is reducible in $R[X]$, that is, $f = f_1 f_2$ for some $f_1, f_2 \in R[X] \smallsetminus R^\times = R[X] \smallsetminus R[X]^\times$, without loss of generality with $\deg(f_1) \leqslant \deg(f_2)$. If $\deg(f_1) = 0$, then $f_1 \in R \smallsetminus R^\times$ divides the greatest common divisor of the coefficients of f, so that f is not primitive. Else, $0 < \deg(f_1) \leqslant \deg(f_2)$ and $f_1, f_2 \in K[X] \smallsetminus K^\times = K[X] \smallsetminus K[X]^\times$, so that f is reducible in $K[X]$. Hence, if f is reducible in $R[X]$, then either it is not primitive or it is reducible in $K[X]$.

   Conversely, assume that if f is not primitive, then $f = c(f) f_0$ for some primitive $f_0 \in R[X]$ and $c(f) \in R \smallsetminus R^\times$. This is a non-trivial factorization of f because $f_0 \notin R[X]^\times$ as it is not constant (its degree coinciding with the one of f) and $c(f) \notin R^\times = R[X]^\times$ by assumption. Moreover, if f is reducible in $K[X]$, i.e., $f = f_1 \cdot f_2$ with $f_i \in K[X]$ with $\deg(f_i) > 0$, by Gauss lemma there exist $\alpha_1, \alpha_2 \in K^\times$ such that $\alpha_1 \alpha_2 = 1$ and $\alpha_i f_i \in R[X]$, so that $f = (\alpha_1 f_1)(\alpha_2 f_2)$ is a non-trivial decomposition of f in $R[X]$. Hence, if f is not primitive or it is reducible in $K[X]$, then f is reducible in $R[X]$.

6. Let $D := XW - YZ \in \mathbb{C}[X, Y, Z, W]$.

   (a) Show that (D) is a prime ideal in $\mathbb{C}[X, Y, Z, W]$. [*Hint:* First, prove that D is an irreducible element]

   (b) Prove that $\mathbb{C}[X, Y, Z, W]/(D)$ is not a UFD. [*Hint:* Let $x = X + (D) \in \mathbb{C}[X, Y, Z, W]/(D)$. Is x prime? Is it irreducible?]

   Solution: We say that a polynomial f (in one or several variables) is *homogeneous of degree d* if all the monomials in f with non-zero coefficients are of degree d. Every polynomial can be uniquely written as a sum of homogeneous polynomials of different degrees.

   (a) Suppose by contradiction that $D = fg$ for some $f, g \in \mathbb{C}[X, Y, Z, W] \smallsetminus \mathbb{C}[X, Y, Z, W]^\times \smallsetminus \{0\} = \mathbb{C}[X, Y, Z, W] \smallsetminus \mathbb{C}$. Then $\deg(f) + \deg(g) = \deg(D) = 2$ and since f and g cannot be constant the only possibility is that $\deg(f) = \deg(g) = 1$. Moreover, $0 = D(0,0,0,0) = f(0,0,0,0)g(0,0,0,0)$ and without loss of generality we can say that $f(0,0,0,0) = 0$ since $\mathbb{C}$ is a domain. This means that f is homogeneous of degree 1. Writing $g = g_1 + g_0$ with g_0 and g_1

homogeneous of degree 0 and 1 respectively, we see that $XW - YZ = D = fg_0 + fg_1$ and since fg_0 is homogeneous of degree 1, we conclude that $fg_0 = 0$ so that $g_0 = 0$ since $f \neq 0$. Hence we can write

$$f = f_X X + f_Y Y + f_Z Z + f_W W, \quad g = g_X X + g_Y Y + g_Z Z + g_W W$$

for some $f_X, f_Y, f_Z, f_W, g_X, g_Y, g_Z, g_W \in \mathbb{C}$. Comparing the coefficients of X^2 in the equality $D = fg$, we see that $f_X g_X = 0$ and without loss of generality, we can assume that $f_X = 0$. Then, comparing the coefficients of XW, we see that $1 = f_X g_W + f_W g_X = f_W g_X$, so that $f_W \neq 0 \neq g_X$. Furthermore, a comparison of the coefficients of XY and XZ gives

$$\begin{aligned} 0 = f_X g_Y + f_Y g_X = f_Y g_X &\implies f_Y = 0 \\ 0 = f_X g_Z + f_Z g_X = f_Z g_X &\implies f_Z = 0, \end{aligned}$$

so that $f = f_W W$ which means that $W | D$, a contradiction (because it would imply that $W | XW - D = YZ$ which cannot hold because of additivity of the degree in W). This implies that D is irreducible. Since $\mathbb{C}[X, Y, Z, W]$ is a UFD ($\mathbb{C}$ is a UFD and for every UFD R, the polynomial ring $R[T]$ is a UFD as seen in class), then D is a prime element, i.e., the ideal (D) is prime.

(b) The given quotient ring is an integral domain because (D) is a prime ideal by part (a). Hence we can talk about irreducible elements. Let $x = X + (D) \in \mathbb{C}[X, Y, Z, W]/(D)$.

The pre-image of the ideal $(x) \subset \mathbb{C}[X, Y, Z, W]/(D)$ under the canonical projection $\mathbb{C}[X, Y, Z, W] \longrightarrow \mathbb{C}[X, Y, Z, W]/(D)$ is $J = (X, XW - YZ) = (X, YZ) \subset \mathbb{C}[X, Y, Z, W]$. Since $Y, Z \notin J$ but $YZ \in J$, the ideal J is not prime, so that $(x) \subset \mathbb{C}[X, Y, Z, W]/(D)$ is not prime by Exercise 5(b) from Assignment 5. This implies that $x \in \mathbb{C}[X, Y, Z, W]/(D)$ is not a prime element.

Suppose that $x = fg$ for some $f, g \in \mathbb{C}[X, Y, Z, W]/(D)$ and take representatives $F, G \in \mathbb{C}[X, Y, Z, W]/(D)$ of f and g respectively. Write $F = F_0 + \cdots + F_n$ and $G = G_0 + \cdots + G_m$ where for each i the polynomials F_i and G_i are homogeneous of degree i. Up to adjusting F and G modulo (D) and reducing the numbers of summands n and m, we may assume that $D \nmid F_n$ and $D \nmid G_m$. The condition $x = fg$ then reads

$$\exists P \in \mathbb{C}[X, Y, Z, W] : X = FG + DP. \tag{2}$$

Writing $P = P_0 + \cdots + P_q$ where P_i is homogeneous of degree i, we notice that $DP = DP_0 + \cdots + DP_q$, where DP_i is homogeneous of degree $i + 2$. In particular, comparing the homogeneous part of degree $n + m$ in the equality (2), we see that if $n + m \geqslant 2$ then

$$0 = F_n G_m + DP_{n+m-2}$$

which implies that $D|F_nG_m$, a contradiction since D is prime by part (a) and $D \nmid F_n, G_m$. Hence $n + m < 2$ and without loss of generality we can assume that $n \leqslant 1$ and $m \leqslant 0$, which implies that $G \in \mathbb{C}[X, Y, Z, W]^\times$ so that $g = G + (D) \in (\mathbb{C}[X, Y, Z, W]/(D))^\times$. Hence x is irreducible.

We proved that x is irreducible but not prime, which as seen in class can only happen if $\mathbb{C}[X, Y, Z, W]/(D)$ is not a UDF.