Exercises 6

Please submit solutions by 3pm on Thursday 22nd March to the pigeonholes in 4W (ground floor).

(W) = Warm-up; (H) = Homework; (A) = Additional.

1. (W) Write the given polynomial as a product of irreducible polynomials in each ring:

(1) $f = 42x^3 - 126x^2 + 84x - 252$ in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$.

(2) $f = x^4 - 5x^2 + 6$ in $\mathbb{Q}[x]$ and $\mathbb{Z}_5[x]$.

2. (H) Let R be an integral domain and let $p \in R$. Show that p is prime if and only if the quotient ring R/Rp is an integral domain.

3. (H) Consider the ring $R = \mathbb{Z}[x]/\langle x^2 + 5\rangle$.

(1) Show that R is an integral domain. [Hint: use the previous question!]

(2) Show that R is not a UFD. [Hint: adapt the proof of Exercise 4.2 to show that R is isomorphic to the ring from Exercise 5.5; this would be straightforward if the coefficients were in $\mathbb{R}$, but having coefficients in $\mathbb{Z}$ makes it more challenging.]

4. (H) Show that $x^3 - 3x - 1$ is irreducible in $\mathbb{Q}[x]$. [Hint: Gauss' Lemma.]

5. (A) Let $\Bbbk$ be a field. For the ring of formal power series $\Bbbk[[x]]$, consider the 'reverse' degree function $\nu\colon \Bbbk[[x]] \smallsetminus \{0\} \to \{0, 1, 2, \ldots\}$ given by $\nu\left(\sum_{i=0}^{\infty} a_i x^i\right) = k$ if $a_i = 0$ for $i < k$ but $a_k \neq 0$.

(1) Show that for $f, g \in \Bbbk[[x]] \setminus \{0\}$, we have $\nu(fg) = \nu(f) + \nu(g)$.

(2) Prove that $\Bbbk[[x]]$ is a Euclidean domain. [Hint: to show part (2) of Definition 3.8 for $f, g \in R[[x]]$ with $g \neq 0$, one can always choose q so that $f = qg$, i.e., $r = 0$.]

The course website is: `http://people.bath.ac.uk/dmjc20/Alg2B/`

---

1. (1) We have $f = 42(x^3 - 3x^2 + 2x - 6)$. By inspecting the integer factors of the constant coefficient -6, we see that 3 is a root of f, and on division by $x - 3$ we get that

$$f = 42(x-3)(x^2+2).$$

The latter factor has no roots in $\mathbb{Q}$, so it's irreducible in both $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$. Note that 42 is a unit in $\mathbb{Q}$, so the above description as the product of a unit with monic, irreducible polynomials is a nice way to write f in $\mathbb{Q}[x]$. However, to present f purely as a product of irreducible factors in $\mathbb{Q}[x]$ we might write

$$f = (42x - 126)(x^2+2),$$

though there are many alternatives (obtained by multiplying the first factor by a nonzero rational number and the second factor by its multiplicative inverse). As for the ring $\mathbb{Z}[x]$, we have

$$f = 2 \cdot 3 \cdot 7 \cdot (x-3)(x^2+2),$$

though again there are many alternatives obtained by multiplying an even number of factors on the right hand side by -1.

(2) For $t = x^2$, first solve $t^2 - 5t + 6 = 0$ and then substitute x back in to see that

$$f = (x^2-2)(x^2-3).$$

None of the roots $\pm\sqrt{2}, \pm\sqrt{3}$ of f in $\mathbb{C}$ lies in $\mathbb{Q}$, so this is the required decomposition in $\mathbb{Q}[x]$. In $\mathbb{Z}_5[x]$, we have that $f = x^4 + 1$, and the result is given in Exercise Sheet 5.

2. ($\Rightarrow$) Assume p is prime. Since R is a commutative ring with 1, Theorem 1.26 shows that R/Rp is a commutative ring with 1. Also, since p is not a unit, we have $Rp \neq R$ and therefore R/Rp is not the zero ring. Finally, suppose that the product of two elemets in R/Rp equals zero, i.e., supose that for $a, b \in R$ we have

$$0 + Rp = (a + Rp) \cdot (b + Rp) = ab + Rp.$$

This means that $ab \in Rp$, or equivalently, that $p|ab$. Since p is prime, it follows that $p|a$ or $p|b$, which means that $a \in Rp$ or $b \in Rp$. Therefore either $a + Rp = 0 + Rp$ or $b + Rp = 0 + Rp$ as required.

($\Leftarrow$) Suppose that R/Rp is an integral domain. Let $a, b \in R$ satisfy $p|ab$. Then

$$(a + Rp) \cdot (b + Rp) = ab + Rp = 0 + Rp,$$

where the last equality follows fomr $p|ab$. Since R is an integral domain, either $a + Rp = 0 + Rp$, in which case $p|a$, or $b + Rp = 0 + Rp$, in which case $p|b$ as required.

3. The polynomial $x^2+5 \in \mathbb{Z}[x]$ is irreducible, because it has no roots in $\mathbb{Z}$. The ring $\mathbb{Z}[x]$ is a UFD because $\mathbb{Z}$ is a UFD, so $x^2 + 5$ is prime by Proposition 3.19. The previous exercise implies that $R = \mathbb{Z}[x]/\langle x^2 + 5\rangle$ is an integral domain.

To see that R is not a UFD, we show that R is isomorphic to the ring $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ from Exercise Sheet 5. Since this latter ring is not a UFD, and since isomorphisms preserve all ring-theoretic properties, it follows that R is not a UFD. To construct the isomorphism, consider the evaluation map

$$\phi\colon \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\sqrt{-5}] \text{ given by } \phi(f) = f(\sqrt{-5}).$$

This is a ring homomorphism by Example 2.6, and it's surjective, since $a + b\sqrt{-5}$ lies in the image of the polynomial $f = a + bx$. We claim that $\mathrm{Ker}(\phi) = \langle x^2 + 5\rangle$, in which case the first isomorphism theorem gives that R is isomorphic to $\mathbb{Z}[\sqrt{-5}]$. To compute the kernel, suppose $f \in \mathbb{Z}[x]$ has degree n and satisfies $f(\sqrt{-5}) = 0$. Regard $f \in \mathbb{R}[x]$ and apply Exercise 5.1 to see that

$$f(x) = (x^2 + 5) \cdot g(x)$$

where $g \in \mathbb{R}[x]$ has degree $n - 2$. Write $g = \sum_{0 \leq i \leq n-2} a_i x^i$. I claim that $a_i \in \mathbb{Z}$. To see this, multiply out the above product and compare coefficients to see that

$$\begin{aligned} a_{n-2} &\in \mathbb{Z} \\ a_{n-3} &\in \mathbb{Z} \\ a_{n-4} + 5a_{n-2} &\in \mathbb{Z} \Rightarrow a_{n-4} \in \mathbb{Z} \\ a_{n-5} + 5a_{n-3} &\in \mathbb{Z} \Rightarrow a_{n-5} \in \mathbb{Z} \end{aligned}$$

and so on, giving $g \in \mathbb{Z}[x]$. Therefore $f \in \langle x^2 + 5 \rangle$, so $\mathrm{Ker}(\phi) \subseteq \langle x^2 + 5 \rangle$. The opposite inclusion is obvious, so $\mathrm{Ker}(\phi) = \langle x^2 + 5 \rangle$. This completes the proof that R is not a UFD.

4. The polynomial $f(x) = x^3 - 3x - 1 \in \mathbb{Z}[x]$ has degree 3, so if it's reducible it would have a factor of degree 1. But -1 only has two integer divisors, neither of which is a root of f. Therefore f is irreducible in $\mathbb{Z}[x]$, so f is irreducible in $\mathbb{Q}[x]$ by Gauss' Lemma.

5. (1) For $f \in \Bbbk[[x]] \setminus \{0\}$ such that $\nu(f) = k$, we can write $f = \sum_{i=k}^{\infty} a_i x^i$ with $a_k \neq 0$. Similarly, for $g \in R[[x]] \setminus \{0\}$ such that $\nu(g) = \ell$, write $g = \sum_{i=\ell}^{\infty} b_i x^i$ with $b_\ell \neq 0$. Then

$$fg = a_k b_\ell x^{k+\ell} + (a_{k+1} b_\ell + a_k b_{\ell+1}) x^{k+\ell+1} + \cdots$$

Since $\Bbbk$ is an integral domain by Remark 1.12, having $a_k \neq 0$ and $b_\ell \neq 0$ forces $a_k b_\ell \neq 0$, so $\nu(fg) = k + \ell = \nu(f) + \nu(g)$.

(2) Part (1) shows that the the first statement of Definition 3.8 holds, namely $\nu(f) \leq \nu(fg)$. As for the second statement, consider again $f = \sum_{i=k}^{\infty} a_i x^i$ with $a_k \neq 0$ and $g = \sum_{i=\ell}^{\infty} b_i x^i$ with $b_\ell \neq 0$. There are two cases:

(a) If $k < \ell$, then $\nu(f) < \nu(g)$, and defining the quotient $q = 0$ and the remainder $r = f$ gives $f = gq + r$ with $\nu(r) < \nu(g)$ as required.

(b) Otherwise, $k \geq \ell$. Consider the power series $g/x^\ell = b_\ell + b_{\ell+1} x + \cdots$. Since $\Bbbk$ is a field, b_ℓ is a unit and therefore the power series g/x^ℓ has an inverse h by Exercise 2.4(1). Notice that $hg = x^\ell$. Now define

$$q = h \cdot \left(a_k x^{k-\ell} + a_{k+1} x^{k-\ell+1} + \cdots \right).$$

Then

$$qg = hg \cdot \left(a_k x^{k-\ell} + a_{k+1} x^{k-\ell+1} + \cdots \right) = x^\ell \cdot \left(a_k x^{k-\ell} + a_{k+1} x^{k-\ell+1} + \cdots \right) = f$$

as required.