MTH6158 Ring Theory: Guide to Coursework 3

Note: This guide is meant to help you understand and carry out the problem solutions on your own. It is **not** meant to provide complete solutions!

1. *In this exercise we will prove that* $\mathbb{Z}[\sqrt{-5}]$ *is an integral domain but not a unique factorisation domain (UFD).*

   (a) *Show that for any integer* m*, the set*

   $$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$$

   is a subring of the field $\mathbb{C}$*. Use this to conclude that* $\mathbb{Z}[\sqrt{m}]$ *is an integral domain.*

   You can prove that $\mathbb{Z}[\sqrt{m}]$ is a subring of $\mathbb{C}$ using the subring test. This implies that $\mathbb{Z}[\sqrt{m}]$ is an integral domain, because if $a, b \in \mathbb{Z}[\sqrt{m}]$ satisfy $a \cdot b = 0$ then, looking at this equation as an equation in $\mathbb{C}$, we conclude that either a or b is zero.

   Note that this argument generalises to show that every subring with identity of an integral domain is an integral domain.

   (b) *Now, let* $S = \mathbb{Z}[\sqrt{-5}]$*. In a similar way to how we computed all the units in the ring of Gaussian integers, prove that if* $u = a + b\sqrt{-5}$ *is a unit of* S *then* $u = 1$ *or* $u = -1$*.*

   Suppose $u = a + b\sqrt{-5}$ is a unit, so there exists $v = c + d\sqrt{-5}$ such that

   $$(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = 1.$$

   Take modulus squared on both sides of this equation to get

   $$(a^2 + 5b^2) \cdot (c^2 + 5d^2) = 1.$$

   As this is an equation about integers, conclude that $a = \pm 1$ and $b = 0$.

   (c) *Note that in* S *we have the following factorisations of the element* 6*:*

   $$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

   It turns out that these are factorisations into irreducible elements. To see this, prove that the element $1 + \sqrt{-5}$ *is irreducible, by assuming that*

   $$1 + \sqrt{-5} = (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) \tag{0.1}$$

and taking modulus squared.

Explain briefly why a similar argument shows that the other three elements $1 - \sqrt{-5}$*,* 2*, and* 3 *are also irreducible.*

This is similar to part (b): Take modulus squared in Equation (0.1), and argue why one of the two factors must be ± 1.

(d) *Conclude that* $\mathbb{Z}[\sqrt{-5}]$ *is not a UFD.*

Part (c) shows that there are elements of $\mathbb{Z}[\sqrt{-5}]$ that can be factored into irreducibles in different non-equivalent ways. Make sure you explain why these two factorisations are really not equivalent up to associates.

2. *Consider the ring* $\mathbb{R}[x]$ *of polynomials with real coefficients.*

(a) *Explain why* $\mathbb{R}[x]$ *is a principal ideal domain.*

The integral domain $\mathbb{R}[x]$ is a principal ideal domain because it is a Euclidean domain. (What is a Euclidean function on it?)

(b) *Give an example of proper non-zero ideals* I_1, I_2, I_3 *of* $\mathbb{R}[x]$ *such that* I_1 *and* I_2 *both contain* I_3*, but* $I_1 \nsubseteq I_2$ *and* $I_1 \nsupseteq I_2$*.*

Every ideal of $\mathbb{R}[x]$ is principal, so we are looking for three polynomials $f_1, f_2, f_3 \in \mathbb{R}[x]$ such that $\langle f_1 \rangle$ and $\langle f_2 \rangle$ both contain $\langle f_3 \rangle$, but $\langle f_1 \rangle \nsubseteq \langle f_2 \rangle$ and $\langle f_1 \rangle \nsupseteq \langle f_2 \rangle$. Think about what this means in terms of divisibility relations among the polynomials f_1, f_2, f_3.

(c) *Find a generator for the ideal* $\langle x^2 - 1, x^3 - 1 \rangle \subseteq \mathbb{R}[x]$*. Explain.*

As $\mathbb{R}[x]$ is a principal ideal domain, the ideal $\langle x^2 - 1, x^3 - 1 \rangle \subseteq \mathbb{R}[x]$ must be generated by a single polynomial f. The polynomial f is in fact the g.c.d. of $x^2 - 1$ and $x^3 - 1$, as discussed in the lectures. Factor the two polynomials to make a guess about what f is, and then prove that $\langle f \rangle$ is the desired ideal.

3. *A non-zero element* p *of a domain* R *is called* **prime** *if* p *is not a unit and whenever* $p \mid a \cdot b$ *for some* $a, b \in R$*, either* $p \mid a$ *or* $p \mid b$*.*

(a) *Prove that every prime element in an integral domain* R *is an irreducible element.*

Suppose that p is not irreducible, so it decomposes as $p = a \cdot b$ with $a, b \in R$ not units. Since $p \mid p$, we have $p \mid a \cdot b$. Use the fact that p is prime to reach a contradiction. Make sure you mention explicitly where you used that R is an integral domain.

(b) *Give an example of a prime element in a domain that is not an irreducible element. Justify your answer.*

The element $[3]_6$ in the ring $\mathbb{Z}_6$ of integers modulo 6 is such an example. You should explain both why it is not an irreducible element and why it is prime.

(c) *Give an example of an irreducible element in the integral domain* $\mathbb{Z}[\sqrt{-5}]$ *that is not a prime element. Justify your answer.*

Think about the factorisations into irreducible elements that you used in Exercise 1.

4. *Let* R *be a Euclidean domain with Euclidean function* d*, and let* $a \in R$ *be a non-zero element.*

(a) *Explain why* $d(a) \geq d(1)$.

This follows directly from the first property of a Euclidean function. Can you see why?

(b) *Prove that* a *is a unit in* R *if and only if* $d(a) = d(1)$.

Think about what happens when you 'divide' 1 by a: There exist q and r such that $1 = a \cdot q + r$ and either $r = 0$ or $d(r) < d(a)$. Use this to prove the desired statement.

5. *In this exercise we will construct and understand the field* $\mathbb{F}_8$ *with 8 elements. Let* $\mathbb{Z}_2$ *be the ring of integers modulo 2, and consider the ring* $R = \mathbb{Z}_2[x]$ *of polynomials with coefficients in* $\mathbb{Z}_2$*. Let* $f = x^3 + x + 1 \in R$.

(a) *Explain why* f *is an irreducible element of* R.

Suppose you can factor $f = g \cdot h$ with $g, h \in R$ not units, so g and h have degree at least 1. Since f has degree 3, one of g and h must have degree 1, say g, and h has degree 2. The polynomial g must have the form $g = x + a$ with $a \in R$, which implies that a is a root of f. However, we can check that $f(0) = f(1) = 1$, so f has no roots in R.

(b) *Conclude that the quotient ring* $F := R/\langle f \rangle$ *is a field.*

Since R is a principal ideal domain and f is irreducible, the ideal $\langle f \rangle$ is a maximal ideal, and thus the factor ring $R/\langle f \rangle$ is a field.

(c) *Explain why every element of* F *can be written uniquely in the form* $[ax^2 + bx + c]$ *with* $a, b, c \in \mathbb{Z}_2$*. Conclude that* F *has exactly* 8 *elements.*

First, note that $[x^3] = [x + 1]$ in F. Using this relation repeatedly, we can express any element $[g(x)] \in F$ with $\deg(g(x)) \geq 3$ as an element of the form $[ax^2 + bx + c]$. To show that this expression is unique, note that two distinct such expressions being the same element in F would imply that $\langle f \rangle$ contains a non-zero polynomial of degree at most 2, which is not possible. This implies that F contains exactly 8 elements, as there are 2 possibilities for each of a, b, c.

(d) *Write down the multiplication table of* F.

Label the 8 rows and columns of the table with the elements of F. Fill the table by multiplying the corresponding elements and reducing the result using the relations discussed in Part 5c.