Exercises 5

HePlease submit solutions by 3pm on Thursday 15th March to the pigeonholes in 4W (ground floor).

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

1. (W) This exercise investigates irreducible polynomials with coefficients in $\mathbb{R}$.

(1) Let $f \in \mathbb{R}[x]$ be nonzero. By repeatedly applying the fundamental theorem of algebra (i.e., every $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$), write f as a product of linear factors in the ring $\mathbb{C}[x]$.

(2) For any non-real root $a \in \mathbb{C}$ of f, show that the complex conjugate $\bar{a}$ is also a root of f, and deduce that the non-real roots of f come in pairs a and $\bar{a}$. Show the polynomial $(x-a)(x-\bar{a})$ has real coefficients, and show that $(x-a)(x-\bar{a})$ is irreducible in $\mathbb{R}[x]$.

(3) Hence write f is a product of irreducible polynomials of degree one and two in the ring $\mathbb{R}[x]$.

2. (W) Factorise the polynomial x^4+1 as a product of irreducibles in $\mathbb{R}[x]$, in $\mathbb{C}[x]$, in $\mathbb{Q}[x]$ and in $\mathbb{Z}_5[x]$. [Hint: you should get four different answers.]

3. (W) Prove that $\mathbb{Q}[x]/\mathbb{Q}[x](x^3-2)$ is a field, and justify your response [Hint: see Theorem 3.17]. Find the inverse of $[x-3]$. [Hint: for the last part, choose $a, b \in \mathbb{Q}$ so that $(x-3)(x^2+ax+b)$ is of the form x^3+c for some $c \in \mathbb{Q}$.]

4. (H) Let $R = \mathbb{Z}[x]$ and consider the ideal $I := R2 + Rx = \{2f + xg \mid f, g \in \mathbb{Z}[x]\}$. Show that I is not a principal ideal of R and conclude that R is an integral domain that is not a PID.

5. (H) Consider the subset $R = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ of $\mathbb{C}$. We investigate some irreducibles that aren't prime.

(1) Show that R is an integral domain. [Hint: prove that it's a subring of $\mathbb{C}$ and apply Lemma 1.20]

(2) Let $N(a) = a \cdot \bar{a}$. Show that $N(ab) = N(a)N(b)$, and hence show that a is a unit in R iff $N(a) = 1$. Use this to determine all the units in R.

(3) Use part (2) to show that $2, 3, 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in R. Use this and

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

to deduce that R is not a UFD and that $2, 3, 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are not primes.

6. (A) Recall that the Gaussian integers $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$ are a subring $\mathbb{C}$. Show that the function $\nu\colon \mathbb{Z}[i] \smallsetminus \{0\} \to \{0, 1, 2, \ldots\}$ given by $\nu(a+bi) = a^2 + b^2$ is a Euclidean valuation, so $\mathbb{Z}[i]$ is a Euclidean domain. [Hint: for $f, g \in \mathbb{Z}[i]$, to find q consider $f/g \in \mathbb{C}$: if it lies in $\mathbb{Z}[i]$ then set $q = f/g$; otherwise let $q \in \mathbb{Z}[i]$ be the point with integer coefficients closest to $f/g \in \mathbb{C}$ in the Argand diagram.]

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

Solutions 5

1. (1) Suppose that $r \in \mathbb{R}$ is the leading coefficient of f, i.e.,

$$f = r\big(x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0\big),$$

where $c_0, \ldots, c_{n-1} \in \mathbb{R}$. Applying the fundamental theorem of algebra repeatedly (you might prove this by induction) gives

$$f = r(x - d_1)\cdots(x - d_n).$$

where $d_1, \ldots, d_n \in \mathbb{C}$.

(2) Suppose that $f(x) = r_0 + r_1 x + \cdots + r_n x^n$. As a is a root of f, we have

$$r_0 + r_1 a + \cdots + r_n a^n = 0.$$

As $\bar{0} = 0$, we get

$$0 = \overline{r_0 + r_1 a + \cdots + r_n a^n} = \overline{r_0} + \overline{r_1 a} + \cdots + \overline{r_n a^n} = r_0 + r_1 \overline{a} + \cdots + r_n \overline{a}^n.$$

Hence $\bar{a}$ is also a root of f. So if a is not real we get a distinct root $\bar{a}$. If $a = r + is$ with $r, s \in \mathbb{R}$ and where $s \neq 0$ then

$$(x - a)(x - \bar{a}) = x^2 - (a + \bar{a})x + a\bar{a} = x^2 - 2rx + (r^2 + s^2)$$

is a polynomial in $\mathbb{R}[x]$. It must be irreducible in $\mathbb{R}[x]$, otherwise it must have a linear factor in $\mathbb{R}[x]$ which is not the case here because neither a nor $\bar{a}$ lies in $\mathbb{R}$.

(3) Let $a_1, \ldots, a_r$ be the real roots of f and let $b_1, \bar{b_1}, \ldots, b_s, \bar{b_s}$ be the non-real roots. If r is the leading coefficient of f we get the factorisation

$$f = r(x - a_1)\cdots(x - a_r)[(x - b_1)(x - \bar{b_1})]\cdots[(x - b_s)(x - \bar{b_s})],$$

which leads to a factorisation in $\mathbb{R}[x]$ with $r+s$ irreducible factors: the r factors $(x-a_1), \ldots, (x-a_r)$ are linear; and the s irreducible factors $(x - b_1)(x - \bar{b_1}), \ldots, (x - b_s)(x - \bar{b_s})$ in $\mathbb{R}[x]$ are quadratic.

2. (1) We have that

$$x^4 + 1 = (x^2 + 1)^2 - 2x^2 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1).$$

As neither of these quadratics has a real root, they are irreducible in $\mathbb{R}[x]$.

(2) We continue with the factorisation from (2) above. We have

$$\begin{aligned} x^4 + 1 &= (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \\ &= \big((x + \tfrac{\sqrt{2}}{2})^2 + \tfrac{1}{2}\big)\big((x - \tfrac{\sqrt{2}}{2})^2 + \tfrac{1}{2}\big) \\ &= (x + \tfrac{\sqrt{2}}{2} + i\tfrac{\sqrt{2}}{2})(x + \tfrac{\sqrt{2}}{2} - i\tfrac{\sqrt{2}}{2})(x - \tfrac{\sqrt{2}}{2} + i\tfrac{\sqrt{2}}{2})(x - \tfrac{\sqrt{2}}{2} - i\tfrac{\sqrt{2}}{2}) \end{aligned}$$

(3) From (1) we know that the unique monic (= leading coefficient is 1) irreducible factors in $\mathbb{R}[x]$ are not in $\mathbb{Q}[x]$. Hence $x^4 + 1$ is irreducible in $\mathbb{Q}[x]$.

(4) We have that $x^4 + 1 = x^4 - 4 = (x^2 + 2)(x^2 - 2)$. Inspection shows that $x^4 + 1$ has no root in $\mathbb{Z}_5$, so we can't factorise further.

3. Since $\mathbb{Q}$ is a field, the ring $\mathbb{Q}[x]$ is a Euclidean domain and hence a PID. The polynomial $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, because a reducible polynomial of degree 3 must have a linear factor, yet none of the roots of $x^3 - 2$ is rational. Theorem 3.16 implies that the quotient ring $\mathbb{Q}[x]/\mathbb{Q}[x](x^3 - 2)$ is a field.

We have

$$[x-3] \cdot [x^2 + 3x + 9] = [x^3 - 27] = [x^3 - 2] + [-25] = [-25],$$

so the inverse of $[x - 3] = [(-1/25)(x^2 + 3x + 9)]$.

4. We argue by contradiction and suppose that

$$R2 + Rx = Rf$$

for some $f \in R = \mathbb{Z}[x]$. In particular, both $2, x \in Rf$, so there exists nonzero polynomials $g_1, g_2 \in \mathbb{Z}[x]$ such that $2 = g_1 f$ and $x = g_2 f$. It follows that $\deg(f) \leq \deg(g_1 f) = \deg(2) = 0$, so f is constant. The only constant polynomials that divide 2 are ± 1 and ± 2, and of these only ± 1 divide x. Therefore $f = 1$ or $f = -1$, so $R \cdot 2 + R \cdot x = R$. It follows that there exists polynomials $r, s \in \mathbb{Z}[x]$ such that

$$1 = 2 \cdot r + x \cdot s.$$

Evaluating at $x = 0$ gives

$$1 = 2 \cdot r(0) + 0 \cdot s(0),$$

and hence $r(0) = \frac{1}{2}$. But $r(0)$ is the constant term of $r(x) \in \mathbb{Z}[x]$, so it must be an integer. This is a contradiction, so the ideal I is not principal. Since $\mathbb{Z}$ is an integral domain, we know from Exercise 2.2(3) that $R = \mathbb{Z}[x]$ is an integral domain, yet we've just shown that R is not a principal ideal domain.

5. (1) Clearly R contains $0 = 0 + 0\sqrt{-5}$, so it's nonempty. We have

$$(a + b\sqrt{-5}) - (c + d\sqrt{-5}) = (a - c) + (b - d)\sqrt{-5} \in R$$

and

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5} \in R$$

for $a, b, c, d \in \mathbb{Z}$, so R is a subring of $\mathbb{C}$. Every field is an integral domain, and since R contains $1 \in \mathbb{C}$, it's an integral domain by Lemma 1.20.

(2) First, note that

$$N(ab) = ab \cdot \overline{ab} = ab\bar{a}\bar{b} = a\bar{a} \cdot b\bar{b} = N(a) \cdot N(b)$$

as required. Next, let $a = r + s\sqrt{-5} \in R$ then $N(a) = r^2 + 5s^2$. Notice that the value is always a non-negative integer. If this is equal to 1 then we must have $r = \pm 1$ and $s = 0$ and we get $a = -1$ or $a = 1$. Clearly both these are units. Conversely suppose that a is a unit and say $ab = 1$ then $1 = N(1) = N(ab) = N(a)N(b)$ and as $N(a), N(b)$ are integers this can only happen if $N(a) = 1$. So 1 and -1 are the only units of R.

(3) First notice that $r^2 + 5s^2$ does not take the values 2 or 3 for any integers r, s. We use this to show that $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible. Firstly if $2 = ab$ then $4 = N(2) = N(a)N(b)$ and as N does not take the value 2 we must have that one of $N(a), N(b)$ takes the value 1 and thus one of a, b must be a unit. This shows that 2 is irreducible. Similarly $3 = ab$ implies that $9 = N(a)N(b)$ and as N does not take the value 3 we must have that one of $N(a), N(b)$ is 1 and thus one of a, b is a unit, so 3 is irreducible. As $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$ the same argument shows that $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible.

The factorisation

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

gives two factorisations of 6 and as 2 doesn't generate the same ideal as either $(1 + \sqrt{-5})$ or $(1 - \sqrt{-5})$, it follows that the factorisation of 6 is not unique. This also shows that none of the four elements is a prime.

6. The map ν clearly takes only nonnegative integer values. For $f = a + bi$ and $g = c + di$ we have

$$\nu(fg) = \nu\big((ac - bd) + (bc + ad)i\big) = (a^2 + b^2)(c^2 + d^2) \geq \nu(f) \quad \text{for } g \neq 0.$$

Now fix $f, g \in \mathbb{Z}[i]$ with $g \neq 0$, and consider the complex number $\frac{f}{g}$. If it is a Gaussian integer then set $q = \frac{f}{g}$ and $r = 0$, so we have $f = qg$. Otherwise, plot the complex number $\frac{f}{g}$ as a point on the Argand diagram representing $\mathbb{C}$ and choose a point $q \in \mathbb{Z}[i]$ such that the real and imaginary parts of the complex number $c := \frac{f}{g} - q$ are at most $\frac{1}{2}$, and define a Gaussian integer $r = f - qg$. We already have $f = qg + r$ with $r \neq 0$, but we must still show that $\nu(r) < \nu(g)$. Since the real and imaginary parts of c are at most $\frac{1}{2}$ we have $|c| \leq \frac{1}{\sqrt{2}}$. Therefore $r = gc$ satisfies

$$\nu(r) = |r|^2 = |g|^2|c|^2 = |c|^2\nu(g) \leq \frac{1}{2}\nu(g) < \nu(g).$$

This shows that ν is a Euclidean valuation.