

1. Which of the following polynomials are irreducible in  $\mathbb{Q}[x]$ ?

(a)  $x^3 - 2x^2 + x - 5$

Since the polynomial  $f(x) = x^3 - 2x^2 + x - 5$  has degree 3, it is irreducible if and only if it has no roots. Since it is monic, every rational root must be an integer that divides the constant term 5. Thus the possible roots are  $\pm 1, \pm 5$ . We test these four possibilities:

$$f(1) = 1 - 2 + 1 - 5 = -5 \neq 0$$

$$f(-1) = -1 - 2 - 1 - 5 = -9 \neq 0$$

$$f(5) = 125 - 50 + 5 - 5 = 75 \neq 0$$

$$f(-5) = -125 - 50 - 5 - 5 = -185 \neq 0$$

Thus  $f(x)$  has no roots, so it is irreducible.

(b)  $x^4 + 3x + 5$

We reduce the polynomial  $f(x) = x^4 + 3x + 5 \pmod{2}$ , to obtain  $\bar{f}(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ .  $\bar{f}(x)$  has no roots, so we use undetermined coefficients to see if it factors:

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd$$

$$a + c = 0, b + d + ac = 0, ad + bc = 1, bd = 1$$

From the last equation we obtain  $b = 1$  and  $d = 1$ , so the first three equations become  $a + c = 0$ ,  $ac = 0$ , and  $a + c = 1$ . The equations  $a + c = 0$  and  $a + c = 1$  are contradictory, so there are no solutions  $a, b, c, d$ . Thus  $\bar{f}(x)$  is irreducible in  $\mathbb{Z}_2[x]$ , and hence  $f(x)$  is irreducible.

(c)  $x^5 + 6x + 15$

We apply the Eisenstein criterion with  $p = 3$ . We have that 3 does not divide 1, 3 divides 6, and 3 divides 15, but 9 does not divide 15, so Eisenstein's criterion implies that  $f(x) = x^5 + 6x + 15$  is irreducible.

2. How many ideals does the ring  $\mathbb{Z}_{12}$  have? List all the ideals of this ring.

From homework we know that  $\mathbb{Z}_m$  is a principal ideal domain. Thus every ideal is generated by a single element. So all the ideals of  $\mathbb{Z}_{12}$  occur in the following list. (We omit the bars over elements of  $\mathbb{Z}_{12}$ .)

$$\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 5 \rangle, \langle 6 \rangle, \langle 7 \rangle, \langle 8 \rangle, \langle 9 \rangle, \langle 10 \rangle, \langle 11 \rangle$$

But there are repetitions in this list. The units of  $\mathbb{Z}_{12}$  are 1, 5, 7, 11, and so each of the ideals  $\langle 1 \rangle, \langle 5 \rangle, \langle 7 \rangle, \langle 11 \rangle$  is the whole ring. Since  $10 = -2$ , we have  $\langle 10 \rangle = \langle 2 \rangle$ . Similarly  $\langle 9 \rangle = \langle 3 \rangle$  and  $\langle 8 \rangle = \langle 4 \rangle$ . Thus there are six ideals in  $\mathbb{Z}_{12}$ :

$$\langle 0 \rangle = \{0\}$$

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$$

$$\langle 3 \rangle = \{0, 3, 6, 9\}$$

$$\langle 4 \rangle = \{0, 4, 8\}$$

$$\langle 6 \rangle = \{0, 6\}$$

3. What are the zero-divisors of the ring  $\mathbb{Z}_3[x]/\langle x^2 + x \rangle$ ?

Let  $R = \mathbb{Z}_3[x]/\langle x^2 + x \rangle$ . Since  $\overline{x^2 + x} = 0$  in  $R$ , we have  $\overline{x^2} = -\overline{x} = \overline{2x}$ , and so every polynomial in  $\mathbb{Z}_3[x]$  is equivalent to a polynomial of degree less than or equal to 2 in  $R$ . Thus there are nine elements in  $R$ :  $\overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2}$ . Now  $x^2 + x = x(x+1)$ , so  $\overline{x(x+1)} = \overline{0}$ , and hence  $\overline{x}$  and  $\overline{x+1}$  are zero-divisors. By definition, a polynomial  $f(x) \in \mathbb{Z}_3[x]$  represents a zero-divisor in  $\mathbb{Z}_3[x]/\langle x(x+1) \rangle$  if and only if  $x(x+1)$  does not divide  $f(x)$ , and there exists  $g(x)$  such that  $x(x+1)$  does not divide  $g(x)$ , but  $x(x+1)$  divides  $f(x)g(x)$ . Since  $\overline{x}$  and  $\overline{x+1}$  are irreducible, this implies  $x$  divides  $f(x)$  or  $x+1$  divides  $f(x)$ . Thus the zero-divisors of  $R$  are  $\overline{x}, \overline{2x}, \overline{x+1}$ , and  $\overline{2x+2}$ .

(An alternate proof is to compute the multiplication table of  $R$  using the relation  $\overline{x^2} = \overline{2x}$ .)

4. (a) If  $f(x)$  is an irreducible polynomial with coefficients in a field  $F$ , explain how to construct a field  $K$  containing  $F$  so that  $f(x)$  has a root in  $K$ . You may use theorems from the course to justify your answer. (Do not reprove the theorems you use.)

We've proved that if  $f(x) \in F[x]$  is irreducible, then the quotient ring  $K = F[x]/\langle f(x) \rangle$  is a field, this field  $K$  contains a root  $\alpha$  of  $f(x)$ , and in fact  $K \cong F[\alpha]$ , the field  $F$  with the root  $\alpha$  adjoined.

(b) Show how this construction works for the polynomial  $x^2 - 5 \in \mathbb{Z}_7[x]$ .

The polynomial  $x^2 - 5 \in \mathbb{Z}_7[x]$  is irreducible, because it has no roots in  $\mathbb{Z}_7$ . (Mod 7 we have  $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 2, 4^2 = 2, 5^2 = 4, 6^2 = 1$ .) Thus the field  $K = \mathbb{Z}_7[x]/\langle x^2 - 5 \rangle$  contains a root of  $f(x) = x^2 - 5$ . In fact, if  $\alpha = \overline{x} \in \mathbb{Z}_7[x]/\langle x^2 - 5 \rangle$ , we have  $f(\alpha) = \overline{x^2 - 5} = \overline{x^2 - 5} = 0 \in K$ . (The field  $K$  also contains the other root  $-\alpha$  of  $f(x)$ .) The isomorphism  $\varphi : K \rightarrow F[\alpha]$  is defined by  $\varphi(\overline{g(x)}) = g(\alpha)$ .

5. Let  $\varphi : \mathbb{Z}[i] \rightarrow \mathbb{Z}_5$  be defined by  $\varphi(a + bi) = \overline{a} + 2\overline{b}$ . Prove that  $\varphi$  is a homomorphism, and use it to prove that  $\mathbb{Z}[i]/\langle 1 + 2i \rangle$  is isomorphic to  $\mathbb{Z}_5$ .

(1)  $\varphi$  is a homomorphism.

$$\varphi(1) = \varphi(1 + 0i) = \overline{1} + 2(\overline{0}) = \overline{1}.$$

$$\varphi((a + bi) + (c + di)) = \varphi((a + c) + (b + d)i) = \overline{a + c} + 2(\overline{b + d}) = \overline{a} + \overline{c} + 2\overline{b} + 2\overline{d} = (\overline{a} + 2\overline{b}) + (\overline{c} + 2\overline{d}) = \varphi(a + bi) + \varphi(c + di).$$

$$\varphi((a + bi)(c + di)) = \varphi((ac - bd) + (ad + bc)i) = \overline{ac - bd} + 2(\overline{ad + bc}) = \overline{ac} - \overline{bd} + 2\overline{ad} + 2\overline{bc} = \overline{ac} + 4\overline{bd} + 2\overline{ad} + 2\overline{bc} = (\overline{a} + 2\overline{b})(\overline{c} + 2\overline{d}) = \varphi(a + bi)\varphi(c + di).$$

(2)  $\varphi$  is surjective.

$$\text{If } \overline{n} \in \mathbb{Z}_5, \text{ then } \varphi(n + 0i) = \overline{n}.$$

(3)  $\ker \varphi = \langle 1 + 2i \rangle$ .

$\varphi(1 + 2i) = \overline{1} + 2(\overline{2}) = \overline{1} + \overline{4} = \overline{5} = \overline{0}$ . Thus  $1 + 2i \in \ker \varphi$ . Now  $|1 + 2i|^2 = 5$ , which is prime, so  $1 + 2i$  is irreducible. Since  $\mathbb{Z}[i]$  is a principal ideal domain, it follows that  $\ker \varphi = \langle 1 + 2i \rangle$ .

Thus  $\varphi$  is a surjective homomorphism with kernel  $\langle 1 + 2i \rangle$ . The Fundamental Homomorphism Theorem gives that  $\mathbb{Z}[i]/\langle 1 + 2i \rangle$  is isomorphic to  $\mathbb{Z}_5$ .