

### Tutorial 6

1. (i) Use the Euclidean Algorithm to show that  $\gcd(23, 14) = 1$  and find integers  $r, s$  such that  $14r + 23s = 1$ . Hence find the inverse of 14 in  $\mathbb{Z}_{23}$ .
- (ii) Let  $I = (x^3 - 2)\mathbb{Q}[x]$ , an ideal in  $\mathbb{Q}[x]$ . Use the Euclidean Algorithm in  $\mathbb{Q}[x]$  to find a polynomial  $f(x) \in \mathbb{Q}[x]$  such that  $f(x) + I$  is the inverse of  $(x^2 - x + 2) + I$  in  $\mathbb{Q}[x]/I$ . Hence express  $\frac{1}{(\sqrt[3]{2})^2 - \sqrt[3]{2} + 2}$  in the form  $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ , with  $a, b, c \in \mathbb{Q}$ .

*Solution.*

(i)  $23 = 1 \times 14 + 9$ ,  $14 = 1 \times 9 + 5$ ,  $9 = 1 \times 5 + 4$ ,  $5 = 1 \times 4 + 1$ , and the next division gives a remainder of 0. The last nonzero remainder gives the gcd; so  $\gcd(23, 14) = 1$ , as claimed. Now working backwards through the above equations we find

$$\begin{aligned} 1 &= 5 - 4 = 5 - (9 - 5) = 2 \times 5 - 9 = 2 \times (14 - 9) - 9 \\ &= 2 \times 14 - 3 \times 9 = 2 \times 14 - 3(23 - 14) = 5 \times 14 - 3 \times 23, \end{aligned}$$

whence  $5 \times 14 \equiv 1 \pmod{23\mathbb{Z}}$ . That is, 5 is the inverse of 14 in  $\mathbb{Z}_{23}$ .

$$\begin{aligned} \text{(ii)} \quad x^3 - 2 &= (x^2 - x + 2)(x + 1) + (-x - 4), \\ x^2 - x + 2 &= (x + 4)(x - 5) + 22. \end{aligned}$$

Thus

$$\begin{aligned} 22 &= (x^2 - x + 2) - (x + 4)(x - 5) \\ &= (x^2 - x + 2) + ((x^3 - 2) - (x^2 - x + 2)(x + 1))(x - 5) \\ &= (x - 5)(x^3 - 2) - (x^2 - 4x - 6)(x^2 - x + 2), \end{aligned}$$

and  $-\frac{1}{22}(x^2 - 4x - 6)(x^2 - x + 2) \equiv 1 \pmod{(x^3 - 2)\mathbb{Q}[x]}$ . Thus  $-\frac{1}{22}(x^2 - 4x - 6) + I$  is the desired inverse. Applying the evaluation homomorphism  $\mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt[3]{2}]$  given by  $x \mapsto \sqrt[3]{2}$  shows that  $22 = -((\sqrt[3]{2})^2 - 4\sqrt[3]{2} - 6)((\sqrt[3]{2})^2 - \sqrt[3]{2} + 2)$ , whence

$$\frac{1}{(\sqrt[3]{2})^2 - \sqrt[3]{2} + 2} = -\frac{1}{22}((\sqrt[3]{2})^2 - 4\sqrt[3]{2} - 6).$$

(By the First Isomorphism Theorem, the evaluation homomorphism gives an isomorphism  $\mathbb{Q}[x]/I \cong \mathbb{Q}[\sqrt[3]{2}]$  such that  $g(x) + I \mapsto g(\sqrt[3]{2})$ , and note that it takes the inverse of  $x^2 - x + 2 + I$  to  $\frac{1}{(\sqrt[3]{2})^2 - \sqrt[3]{2} + 2}$ .)

2. Find the unique monic polynomial  $d(x) \in \mathbb{F}_2[x]$  that is a greatest common divisor of  $r(x) = x^4 + x^3 + x^2 + 1$  and  $s(x) = x^3 + 1$ . Find polynomials  $a(x)$  and  $b(x)$  in  $\mathbb{F}_2[x]$  such that  $d(x) = a(x)r(x) + b(x)s(x)$ .

*Solution.*

Use the Euclidean Algorithm. Remembering that  $-1 = 1$  in characteristic 2, we find that

$$\begin{aligned} x^4 + x^3 + x^2 + 1 &= (x + 1)(x^3 + 1) + x^2 + x, \\ x^3 + 1 &= (x + 1)(x^2 + x) + x + 1, \\ x^2 + x &= x(x + 1). \end{aligned}$$

The gcd has to be a scalar multiple of the last nonzero remainder. So  $d(x) = x + 1$ .

Working back through the equations above, we obtain

$$\begin{aligned} x + 1 &= x^3 + 1 + (x + 1)(x^2 + x) = s(x) + (x + 1)r(x) + (x + 1)s(x) \\ &= (x + 1)r(x) + x^2s(x). \end{aligned}$$

Thus  $a(x) = x + 1$  and  $b(x) = x^2$  is a solution.

3. (i) Find all irreducible quadratics, cubics and quartics in  $\mathbb{F}_2[x]$ .
- (ii) Find all irreducible monic quadratic and cubics in  $\mathbb{F}_3[x]$ .

*Solution.*

Testing for linear factors by substitution identifies the reducible quadratics and cubics. A reducible quartic will either have a linear factor or be the product of irreducible quadratics.

- (i) In  $\mathbb{F}_2[x]$  there is 1 irreducible quadratic  $x^2 + x + 1$ , 2 irreducible cubics  $x^3 + x + 1$ ,  $x^3 + x^2 + 1$  and 3 irreducible quartics  $x^4 + x + 1$ ,  $x^4 + x^3 + 1$ , and  $x^4 + x^3 + x^2 + x + 1$ .
- (ii) There are three irreducible quadratics  $x^2 + 1$ ,  $x^2 \pm x - 1$  and 8 irreducible cubics  $x^3 - x + 1$ ,  $x^3 + x^2 - x + 1$ ,  $x^3 - x^2 + 1$ ,  $x^3 - x^2 + x + 1$ ,  $x^3 - x - 1$ ,  $x^3 + x^2 - 1$ ,  $x^3 + x^2 + x - 1$ ,  $x^3 - x^2 - x - 1$ .

4. Let  $R$  be a principal ideal domain. Show direct from the definitions that a non-zero  $\pi \in R$  is irreducible if and only if  $\pi R$  is a maximal ideal.

*Solution.*

Let  $R$  be an arbitrary integral domain. A non-zero element  $\pi \in R$  is irreducible if it is not a unit and  $a|\pi$  implies  $a$  is an associate of  $\pi$  or  $a$  is a unit. We can express these conditions in terms of ideals:  $\pi \in R$  is irreducible if  $\pi R \neq R$  and  $\pi R \subseteq aR$  implies  $aR = \pi R$  or  $aR = R$ . [Lecture 16, Observation 16.2]. This says  $\pi$  is irreducible if and only if  $\pi R$  is a maximal principal ideal. So if  $R$  is a principal ideal domain,  $\pi$  is irreducible if and only if  $\pi R$  is a maximal ideal.

5. Let  $\mathbb{G} = \{n + mi \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{C}$ , the ring of *Gaussian integers*.

- (i) List all the elements of the quotient ring  $S = \mathbb{G}/3\mathbb{G}$ , and write out complete addition and multiplication tables for  $S$ .
- (ii) Use your multiplication table to show that every nonzero element of  $S$  has a multiplicative inverse, and deduce that  $S$  is a field.

*Solution.*

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+i}$	$\overline{2i}$	$\overline{1+2i}$	$\overline{2+2i}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+i}$	$\overline{2i}$	$\overline{1+2i}$	$\overline{2+2i}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\overline{1+i}$	$\overline{2+i}$	$\bar{i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\overline{2i}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\overline{2+i}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+2i}$	$\overline{2i}$	$\overline{1+2i}$
$\bar{i}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+i}$	$\overline{2i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\overline{1+i}$	$\overline{1+i}$	$\overline{2+i}$	$\bar{i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\overline{2i}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\overline{2+i}$	$\overline{2+i}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+2i}$	$\overline{2i}$	$\overline{1+2i}$	$\bar{2}$	$\bar{0}$	$\bar{1}$
$\overline{2i}$	$\overline{2i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+i}$
$\overline{1+2i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\overline{2i}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\overline{1+i}$	$\overline{2+i}$	$\bar{i}$
$\overline{2+2i}$	$\overline{2+2i}$	$\overline{2i}$	$\overline{1+2i}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\overline{2+i}$	$\bar{i}$	$\overline{1+i}$

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+i}$	$\overline{2i}$	$\overline{1+2i}$	$\overline{2+2i}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{i}$	$\overline{1+i}$	$\overline{2+i}$	$\overline{2i}$	$\overline{1+2i}$	$\overline{2+2i}$
$\bar{2}$	$\bar{2}$	$\bar{1}$	$\overline{2i}$	$\overline{2+2i}$	$\overline{1+2i}$	$\bar{i}$	$\overline{2+i}$	$\overline{1+i}$
$\bar{i}$	$\bar{i}$	$\overline{2i}$	$\bar{2}$	$\overline{2+i}$	$\overline{2+2i}$	$\bar{1}$	$\overline{1+i}$	$\overline{1+2i}$
$\overline{1+i}$	$\overline{1+i}$	$\overline{2+2i}$	$\overline{2+i}$	$\overline{2i}$	$\bar{1}$	$\overline{1+2i}$	$\bar{2}$	$\bar{i}$
$\overline{2+i}$	$\overline{2+i}$	$\overline{1+2i}$	$\overline{2+2i}$	$\bar{1}$	$\overline{2+i}$	$\overline{1+i}$	$\overline{2i}$	$\bar{2}$
$\overline{2i}$	$\overline{2i}$	$\bar{i}$	$\bar{1}$	$\overline{1+2i}$	$\overline{1+i}$	$\bar{2}$	$\overline{2+2i}$	$\overline{2+i}$
$\overline{1+2i}$	$\overline{1+2i}$	$\overline{2+i}$	$\overline{1+i}$	$\bar{2}$	$\overline{2i}$	$\overline{2+2i}$	$\bar{i}$	$\bar{1}$
$\overline{2+2i}$	$\overline{2+2i}$	$\overline{1+i}$	$\overline{1+2i}$	$\bar{i}$	$\bar{2}$	$\overline{2+i}$	$\bar{1}$	$\overline{2i}$

An arbitrary element  $\alpha \in \mathbb{G}/3\mathbb{G}$  has the form  $n + mi + 3\mathbb{G}$ , where  $n, m \in \mathbb{Z}$ . Dividing by 3, we can find quotients  $p, q \in \mathbb{Z}$  and remainders  $r, s \in \{0, 1, 2\}$  such that  $n = 3p + r$  and  $m = 3q + s$ . This gives  $\alpha = n + mi + 3\mathbb{G} = r + si + 3\mathbb{G}$ , since  $(n + mi) - (r + si) = 3(p + qi) \in 3\mathbb{G}$ . Since there are only 3 choices for  $r$  and 3 choices for  $s$  we see that  $\mathbb{G}/3\mathbb{G}$  has at most 9 distinct elements. Using the notation  $\overline{n + mi}$  for  $n + mi + 3\mathbb{G}$ , the elements are  $\bar{0}, \bar{1}, \bar{2}, \bar{i}, \overline{1+i}, \overline{2+i}, \overline{2i}, \overline{1+2i}, \overline{2+2i}$ . It is easily seen that these 9 elements are all different, since if  $r, r', s, s' \in \{0, 1, 2\}$  and  $\overline{r + si} = \overline{r' + s'i}$  then  $r - r'$  and  $s - s'$  must both be divisible by 3, and this forces  $r = r'$  and  $s = s'$  (given that  $r, r', s, s' \in \{0, 1, 2\}$ ).

Routine calculations yield the tables shown. Observe that  $\bar{1}$  appears in every row of the multiplication table of the nonzero elements, which shows that every element has a right inverse. (An element  $y$  is a right inverse of an element  $x$  if  $xy$  is the identity,

a left inverse if  $yx$  is the identity, and an inverse if both a right inverse and a left inverse.) In this case the ring is commutative, and so a right inverse is necessarily an inverse. Hence  $S$  is a commutative ring with identity such that all nonzero elements have inverses; that is, a field.