

### Tutorial 7

1. Let  $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ , a subdomain of  $\mathbb{C}$ . Define a norm function on  $R$  by  $N(a + b\sqrt{-5}) = a^2 + 5b^2$ .
  - (i) Show that  $N(\alpha\beta) = N(\alpha)N(\beta)$ , for all  $\alpha, \beta \in R$ .
  - (ii) Show that  $\alpha \in R$  is a unit if and only if  $N(\alpha) = 1$ , and hence find all the units of  $R$ .
  - (iii) Find all elements of  $R$  with  $N(\alpha) \leq 6$ .
  - (iv) Which of the following elements are primes of  $R$  and which are irreducible?  
 $2, 3, 4, 1 + \sqrt{-5}, 1 - \sqrt{-5}$
  - (v) What are the irreducible divisors of 6 in  $R$ ?
  - (vi) Show that the elements 6 and  $2(1 + \sqrt{-5})$  have no gcd in  $R$ .

#### Solution.

(i) Note that  $N(\alpha) = \alpha\bar{\alpha}$ , where “ $\bar{\phantom{x}}$ ” denotes complex conjugation. We have  

$$N(\alpha\beta) = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta).$$

(ii) Let  $\alpha = a + b\sqrt{-5}$ , and suppose first that  $N(\alpha) = 1$ . Then  $a^2 + 5b^2 = 1$ , and clearly the only solutions of this are given by  $b = 0$  and  $a = \pm 1$ . So  $\alpha = \pm 1$ . In either case  $\alpha$  has an inverse: indeed, 1 is the inverse of 1 and  $-1$  the inverse of  $-1$ . So all elements of norm 1 are units.

Conversely, if  $\alpha$  is a unit then there is  $\beta \in R$  such that  $\alpha\beta = 1$ . This implies that  $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$ . Since  $N(\alpha)$  and  $N(\beta)$  are positive integers it follows that  $N(\alpha) = 1$ .

Thus all units have norm 1, and the only units in  $R$  are 1 and  $-1$ .

(iii) The elements of norm  $k$  have the form  $a + b\sqrt{-5}$ , where  $a, b \in \mathbb{Z}$  satisfy  $a^2 + 5b^2 = k$ . Clearly 0 is the only element of norm 0, and we have already found that the only elements of norm 1 are  $\pm 1$ . It is easily seen that  $a^2 + 5b^2 = 2$  has no solution in integers  $a, b$ . So there are no elements  $\alpha \in R$  with  $N(\alpha) = 2$ . Similarly, there no  $\alpha \in R$  with  $N(\alpha) = 3$ . The elements with  $N(\alpha) = 4$  are  $\pm 2$ ; the elements with  $N(\alpha) = 5$  are  $\pm\sqrt{-5}$ ; the elements with  $N(\alpha) = 6$  are  $\pm 1 \pm \sqrt{-5}$ .

(iv) Suppose that  $\alpha, \beta \in R$ . To say that  $\alpha|\beta$  means that  $\beta = \alpha\gamma$  for some  $\gamma \in R$ . If this holds then  $N(\beta) = N(\alpha)N(\gamma)$ , by Part (i). Note that this is now an equation in positive integers. We have shown that  $\alpha|\beta$  (in  $R$ ) implies that  $N(\alpha)|N(\beta)$  (in  $\mathbb{Z}$ ). Note also that if  $\alpha|\beta$  and  $N(\alpha) = N(\beta)$  then the element  $\gamma \in R$  satisfying  $\beta = \alpha\gamma$  must have norm 1; so  $\gamma = \pm 1$ , and  $\alpha = \pm\beta$ .

Since 4 has an obvious factorisation (as  $2^2$ ) with factors that are not units or associates of 4, it is clear that 4 is not irreducible. The elements 2, 3,  $1 + \sqrt{-5}$  and  $1 - \sqrt{-5}$  are irreducible. For example, if  $\alpha \in R$  and  $\alpha|3$  then  $N(\alpha)|N(3) = 9$ , and so  $N(\alpha) = 1$  or  $N(\alpha) = 9$ , since there are no elements of norm 3. So the only divisors of 3 in  $R$  are  $\pm 1$  and  $\pm 3$ . Similarly, if  $\alpha|(1 + \sqrt{-5})$  then  $N(\alpha)|6$ , so that  $N(\alpha)$  is 1 or 6, since there are no elements of norm 2 or 3. So the only divisors of  $1 + \sqrt{-5}$  are  $\pm 1$  and  $\pm(1 + \sqrt{-5})$ . Similar arguments work for 2 and  $1 - \sqrt{-5}$ .

Recall that in an arbitrary integral domain an element  $p$  is said to be prime if  $p|ab$  implies  $p|a$  or  $p|b$ . For PID's all irreducibles are prime and vice versa; however, in general irreducible does not imply prime, although prime does imply irreducible.

None of the listed elements are prime. The one that is not irreducible is obviously not prime:  $4|2^2$  but  $4 \nmid 2$ . For the others, the key is to observe that  $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \times 3$ . So  $2|(1 + \sqrt{-5})(1 - \sqrt{-5})$ , but obviously  $2 \nmid (1 + \sqrt{-5})$  and  $2 \nmid (1 - \sqrt{-5})$  since  $1 + \sqrt{-5}$  and  $1 - \sqrt{-5}$  are irreducible. Similarly,  $(1 + \sqrt{-5})|2 \times 3$ , but  $(1 + \sqrt{-5}) \nmid 2$  and  $(1 + \sqrt{-5}) \nmid 3$ .

(v) Let us find all possible factorisations of 6 in  $R$ . Suppose that  $6 = \alpha\beta$ , choosing the notation so that  $N(\alpha) \leq N(\beta)$ . By Part (i),  $36 = N(\alpha)N(\beta)$ , and using Part (iii) we see that the only possible values of  $N(\alpha)$  are 1, 4 and 6. So by Part (iii) it follows that the possible values of  $\alpha$  are  $\pm 1, \pm 2$  and  $\pm 1 \pm \sqrt{-5}$ . So the only nontrivial factorisations of 6 are the two we have seen, namely  $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3$ , and the two others obtained by multiplying both factors by  $-1$ . So the only irreducible factors of 6 are  $\pm 2, \pm 3$  and  $\pm 1 \pm \sqrt{-5}$ .

(vi) Suppose that  $d = \gcd(6, 2(1 + \sqrt{-5}))$ . Then  $d$  is a common divisor of 6 and  $2(1 + \sqrt{-5})$ ; so  $d|6$  and  $d|1 + \sqrt{-5}$ , and so  $N(d)|36$  and  $N(d)|24$  (since  $N(6) = 36$  and  $N(2(1 + \sqrt{-5})) = 24$ ). On the other hand, since  $d$  is a *greatest* common divisor of 6 and  $2(1 + \sqrt{-5})$  and other common divisor must be a divisor of  $d$ . Now  $2|6$  and  $2|2(1 + \sqrt{-5})$ ; so  $2|d$ . And  $1 + \sqrt{-5}$  also divides both 6 and  $2(1 + \sqrt{-5})$ ; so  $(1 + \sqrt{-5})|d$ . Taking norms gives  $4|N(d)$  and  $6|N(d)$ . The only positive integer satisfying the four conditions we have obtained is  $N(d) = 12$ . If  $d = a + b\sqrt{-5}$  then  $a^2 + 5b^2 = 12$ . However, no integers  $a$  and  $b$  satisfying this equation exist; so 6 and  $2(1 + \sqrt{-5})$  do not have a gcd. (So  $R$  cannot be a PID!)

2. Let  $F$  be a field, and let  $f \in F[x]$  be a non-zero polynomial over  $F$ . Recall an element  $a \in F$  is a *root* of  $f$  in  $F$  if  $f(a) = 0$ , and this is the case if and only if  $x - a$  divides  $f(x)$  in  $F[x]$ . A root is said to have multiplicity  $m$  if  $(x - a)^m | f(x)$ , but  $(x - a)^{m+1} \nmid f(x)$ .
  - (i) Find all roots of the polynomials  $x^2 - 1$  and  $x^2 - x$  in  $F$ .
  - (ii) Prove that if  $f$  is a nonzero polynomial of degree  $n$ , then  $f$  has at most  $n$  roots in  $F$ .
  - (iii) Deduce if  $f(x), g(x) \in F[x]$  both of degree less than or equal to  $n$  take the same value at more than  $n$  distinct points then  $f(x) = g(x)$ .

*Solution.*

(i) If  $t$  is a root of  $x^2 - 1$ , then  $t^2 - 1 = 0$ , and so  $(t - 1)(t + 1) = 0$ . This gives  $t - 1 = 0$  or  $t + 1 = 0$ , since fields have no zero divisors. Hence  $\pm 1$  are the only possible roots. Conversely, it is obvious that  $\pm 1$  are roots. Note that if  $F$  has characteristic 2,  $1 = -1$  is a double root.

In any field,  $1^2 - 1 = 0$  and  $0^2 - 0 = 0$ . So 1 and 0 are certainly roots of  $x^2 - x$ . Conversely, suppose that  $t$  is a root of  $x^2 - x$ . Then  $0 = t^2 - t = t(t - 1)$ , and so  $t - 1 = 0$  or  $t = 0$ . Hence  $t = 1$  or  $t = 0$ .

(ii) Use induction on the degree of the polynomial. Consider a polynomial  $f$  of degree 0. Thus  $f$  is a nonzero constant, and so  $f(t) \neq 0$  for all  $t$ . So  $f$  has no roots, thus the number of roots of  $f$  is at most 0, the degree of  $f$ , as required.

Suppose, inductively, that every polynomial of degree  $n$  has at most  $n$  roots (for some  $n \geq 0$ ), and let  $f$  be a polynomial of degree  $n + 1$ . If  $f$  has no roots, then since  $0 \leq n + 1$ , we are done. So suppose that  $f$  has a root, say  $t$ . By division of polynomials we have  $f = (x - t)g + r$ , for some polynomials  $g$  and  $r$ , with  $r$  of degree less than  $\deg(x - t) = 1$ . Thus  $r$  is a constant. Putting  $x = t$  in this relation gives  $r = 0$ , since  $t$  is a root of  $f$ . Thus  $f = (x - t)g$ . Taking degrees of both sides, we find that  $\deg g = n$ , and so  $g$  has at most  $n$  roots, by the inductive hypothesis. We now aim to show that every root of  $f$  is either  $t$  or a root of  $g$ , and hence that  $f$  has at most  $n + 1$  roots.

Let  $s$  be a root of  $f$ , so that  $f(s) = 0$ . Then  $0 = f(s) = (s - t)g(s)$ . Since  $F$  is a field, either  $s - t = 0$  or  $g(s) = 0$ . In the former case, we have  $s = t$ , and in the latter case  $s$  is a root of  $g$ . Hence every root of  $f$  is either  $t$  or a root of  $g$ , and the result follows.

3. Express each of the following polynomials in  $\mathbb{Z}_2[x]$  as a product of irreducibles:  $x^4 + x^3 + x^2 + 1$  and  $x^4 + x^2 + 1$ .

*Solution.*

Note that  $x = 1$  is a root of  $x^4 + x^3 + x^2 + 1$ ; so  $x + 1$  is a factor. Dividing gives  $x^4 + x^3 + x^2 + 1 = (x + 1)(x^3 + x + 1)$ . Both factors are irreducible. The polynomial  $x^4 + x^2 + 1$  has no roots; so it has no factors of degree 1. Thus, it can only be an irreducible itself, or the square of  $x^2 + x + 1$ . The latter turns out to be the case:  $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ .

4. Let  $E$  be the ring obtained from  $\mathbb{Z}_2$  by adjoining an element  $\alpha$  that is a root of the polynomial  $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ .

- (i) What theorem from the course guarantees that  $E$  is a field? Check that the hypotheses of this theorem are satisfied.
- (ii) Find, by trial and error, all the roots in  $E$  of  $x^7 - 1 \in E[x]$ . (The observation that any power of a 7th root of 1 is also a 7th root of 1 may be useful.) Express  $x^7 - 1$  as a product of polynomials in  $E[x]$  which are irreducible.

- (iii) What are the irreducible factors of  $x^7 - 1$  in  $\mathbb{Z}_2[x]$  (rather than  $E[x]$ )?

*Solution.*

The theorem says that whenever  $F$  is a field and  $p(x) \in F[x]$  is irreducible then adjoining a root of  $p(x)$  to  $F$  gives a field that has  $F$  as a subfield. This in turn comes from the theorem that adjoining a root of  $p(x)$  to  $E$  produces a ring isomorphic to  $F[x]/p(x)F[x]$ , combined with the theorem that  $R/pR$  is a field whenever  $R$  is a PID and  $p \in R$  is irreducible.

To confirm that the theorem applies we just need to check that the polynomial  $x^3 + x + 1 \in \mathbb{Z}_2[x]$  is irreducible. For this see Tutorial 6, **Q3**.

All elements of  $E$  can be expressed in the form  $a + b\alpha + c\alpha^2$ , with  $a, b, c \in \mathbb{Z}_2$ . This is because  $\alpha^3 + \alpha + 1 = 0$  gives  $\alpha^3 = \alpha^2 + 1$  (since  $1 = -1$  in characteristic 2), enabling powers of  $\alpha$  higher than the 2nd power to be expressed in terms of  $\alpha^0$ ,  $\alpha^1$  and  $\alpha^2$ .

You were asked to use trial and error to find which of these 8 elements  $t$  satisfy  $t^7 = 1$ . It seems natural to try  $t = \alpha$  first. In fact, the nonzero elements of  $E$  form a group under multiplication, and since this group has 7 elements a theorem of group theory (Lagrange's Theorem) guarantees that they all satisfy  $t^7 = 1$ .

We find that the powers of  $\alpha$  are  $\alpha, \alpha^2, \alpha^3 = \alpha^2 + 1, \alpha^4 = (\alpha^2 + 1) + \alpha = \alpha^2 + \alpha + 1, \alpha^5 = (\alpha^2 + 1) + \alpha^2 + \alpha = \alpha + 1, \alpha^6 = \alpha^2 + \alpha$  and  $\alpha^7 = (\alpha^2 + 1) + \alpha^2 = 1$ . So the nonzero elements of  $E$  are all powers of  $\alpha$ . Now  $(\alpha^i)^7 = (\alpha^7)^i = 1^i = 1$  for all positive integers  $i$ ; so  $\alpha^i$  is a root of  $x^7 - 1$  for each  $i$ . So  $1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha$  and  $\alpha^2 + \alpha + 1$  are all roots of  $x^7 - 1$ . Now if  $t$  is a root of a polynomial  $f(x)$  then  $x - t$  is a factor of  $f(x)$ , and indeed it is not hard to check by direct calculation that  $x^7 - 1 = (x - 1)(x - \alpha)(x - \alpha + 1)(x - \alpha^2)(x - \alpha^2 + 1)(x - \alpha^2 + \alpha)(x - \alpha^2 + \alpha + 1)$ .

As  $x^3 + x^2 + 1$  is irreducible in  $\mathbb{Z}_2[x]$  the gcd of  $x^3 + x + 1$  and  $x^7 + 1$  is either  $x^3 + x^2 + 1$  or 1. If it is 1 then there exist  $r(x)$  and  $s(x)$  with  $r(x)(x^3 + x + 1) + s(x)(x^7 + 1) = 1$ . But in  $E[x]$  we have  $x + \alpha \mid x^3 + x^2 + 1$  and  $x + \alpha \mid x^7 + 1$ ; so  $x + \alpha \mid 1$ , which is absurd. So  $x^3 + x^2 + 1$  must be a factor of  $x^7 + 1$ . This is easily checked:

$$\begin{aligned} x^7 + 1 &= (x + 1)(x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1) \\ &= (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1). \end{aligned}$$

Observe that these factors are irreducible in  $\mathbb{Z}_2[x]$ . Checking the factorisation of  $x^7 + 1$  in  $E(x)$  is now easier, since we find readily that

$$x^3 + x + 1 = (x + \alpha)(x^2 + \alpha x + \alpha^2 + 1) = (x + \alpha)(x + \alpha^2)(x + \alpha^2 + \alpha),$$

and

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