

### 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?

$$2, \quad 3, \quad 4, \quad 1 + \sqrt{-5}, \quad 1 - \sqrt{-5}$$

- (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  $R$ .

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  $(x - a)^m \mid f(x)$ , 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  $f(x) = g(x)$ .

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  $x^4 + x^2 + 1$ .

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  $E[x]$ )?