

**Exercises 4**

1. Consider the irreducible polynomial  $X^2+1$  defined over  $\mathbb{F}_3 := \mathbb{Z}_3$  and construct the field  $F := \mathbb{F}_3[X]/\langle X^2 + 1 \rangle$ . Show that  $(F^\times, \cdot)$  is a cyclic group and write down its multiplicative table.
  2. Make a list of the irreducible polynomials of degree less than or equal to 4 when considered over  $\mathbb{F}_2$ . Do the same up until degree 3, when defined over  $\mathbb{F}_3$ .
  3. Examine the coset of  $X$  in the field  $\mathbb{F}_{16} := \mathbb{F}_2[X]/\langle X^4 + X + 1 \rangle$ . Show that the coset  $\overline{X}$  generates  $(\mathbb{F}_{16}^\times, \cdot)$ , confirming that it is a cyclic group.
  4. Describe the factor ring  $\mathbb{Q}[X]/\langle X^2 - 1, X^3 + X \rangle$ .
  5. Determine how many elements the factor ring  $E = \mathbb{F}_5[X]/\langle X^3 - X + a \rangle$  for  $a \in \mathbb{F}_5 = \mathbb{Z}_5$ . Decide for which values of  $a$ ,  $E$  is a field.
  6. *Doubling the cube.* Given a cube of volume 1 show that it is impossible to construct a cube of volume 2 using a straightedge and compass.
  7. *Squaring the circle.* Given a circle of radius 1 show that it is impossible to construct a square of the same area using a straightedge and compass.
-