Introduction to Homomorphic Cryptosystems
Exercise Sheet 3: Polynomial Rings

Task 1 – Rings

Show that the following structures satisfy the ring axioms and are therefore rings.

a) The definition of polynomial rings from the lecture.

b) The set of 2-by-2 square matrices ($M_2(R)$) with entries in a ring R together with matrix multiplication and matrix addition.

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in R \right\}$$

Task 2 – Reducibility

In the lecture we defined the term reducibility in the context of polynomials. For this task we give a more concrete definition:

Let R be an integral domain (nonzero commutative ring) and let p be a non-zero non-unit in $R[X]$, we say that p is reducible over R if we can factor $p = gh$ where both g and h are non-units. Otherwise we say that p is irreducible over R.

The definition of a unit is:

A unit of a ring is an invertible element for the multiplication of the ring. That is, an element u of a ring R is a unit if there exists v in R such that $vu = uv = 1$ where 1 is the multiplicative identity.

Now decide for the following polynomials if they are reducible over the corresponding domains

a) $2x + 2$ over $\mathbb{Z}$

b) $2x + 2$ over $\mathbb{R}$

c) $x^2 - 5$ over $\mathbb{R}$

d) $x^2 - 5$ over $\mathbb{Q}$

Task 3 – Polynomial division

Give a short description on how to calculate the remainder when given any polynomial p and a modulus m. You can describe the process by writing down the steps (pseudo code like).

Task 4 – Root of unity

Proof the following theorems:

a) If x is a n-th root of unity, then so is x^k, where $k \in \mathbb{Z}$.

b) If z is a n-th root of unity and $a \equiv b \pmod{n}$ then $z^a = z^b$.

c) If z is a n-th root of unity and $z^a = z^b$, then $a \equiv b \pmod{n}$ may be false.