46) (GAP, followup on problem 45) The following polynomials are irreducible (i.e. have no proper factors of degree \( \geq 1 \)) over the field \( \mathbb{Z}_2 \):

\[
    x^2 + x + 1, \quad x^3 + x + 1, \quad x^4 + x + 1
\]

The corresponding quotient rings \( Q := \mathbb{Z}_2[x]/(p(x)) \) therefore are fields (with respectively 4, 8 and 16 elements). For each of these fields \( Q \) (with \( 2^n \) elements) show (by trying out multiplication of elements in \( Q \)) that there is an element \( \alpha \in Q \) such that \( \alpha^{2^n-1} = 1 \) but \( \alpha^m \neq 1 \) for all \( 0 < m < 2^n - 1 \). (Such an element \( \alpha \) is a primitive root. All finite fields have primitive roots, which will be shown later. Primitive roots are important in many applications. When creating finite fields in GAP, it actually represents all nonzero elements as powers of a primitive root. See for example the output of the command \texttt{Elements(GF(8))}; which will list all elements of the field with 8 elements.)

47) Let \( R, S \) be rings and \( \varphi: R \to S \) a homomorphism that is onto (i.e. \( \varphi(R) = S \)).

a) Let \( A \triangleleft R \). Show that \( \varphi(A) = \{ \varphi(a) \mid a \in A \} \triangleleft S \).

b) Let \( B \triangleleft S \). We consider \( A := \{ a \in R \mid \varphi(a) \in B \} \). (This is called the full preimage of \( B \).) Show that \( A \triangleleft R \) and that \( A = \varphi(A) \).

c) Now consider the case that \( S = R/J \) for an ideal \( J \triangleleft R \) and \( \varphi: R \to S \) the natural homomorphism. Show that the ideals of \( S \) are exactly of the form \( \varphi(A) \) for \( J \leq A \triangleleft R \). (I.e. the ideals of \( R/J \) are determined by the ideals of \( R \) which contain \( J \). Compare problem 45.)

48) Construct (via an appropriate quotient of \( \mathbb{Q}[x, y] \)) a commutative ring \( R \) in which

- There is a subring \( S \leq R \) which is isomorphic to the rational numbers.

- There are two elements \( x \) and \( y \) such that \( x^2 = y^2 = -1 \) but \( x \neq y \) and \( x \neq -y \). (I.e. we have four different square roots of \(-1\))

Is this ring \( R \) an integral domain?

49) (GAP) The message \( \alpha, \alpha, \alpha, \alpha^4, \alpha^2, \alpha^3, \alpha^2 \), encoded in the Reed-Solomon code over the field with 8 elements as presented in the lecture has been received. Decode this message.

50) (GAP) Construct the Reed-Solomon code (e.g. a generator matrix and syndromes) for the field with 9 elements. You may get the elements of this field in GAP by the command \texttt{Elements(GF(9))}.

51) Over the ring \( \mathbb{Z}_2 \) the polynomial \( x^{15} - 1 \) factors as

\[
    x^{15} - 1 = x + 1 \cdot x^2 + x + 1 \cdot x^4 + x + 1 \cdot x^4 + x^3 + 1 \cdot x^4 + x^3 + x^2 + x + 1.
\]

How many cyclic codes of length 15 with coefficients in \( \mathbb{Z}_2 \) exist?

Problems marked with a * are bonus problems for extra credit.