UE Discrete Mathematics

Exercises for Jan 22/23, 2014

111) Let K be a field. Prove:

(a) If $a, b \in K$, then for all $k, l \in \mathbb{N}^+$ the element $\sqrt[k]{a}\sqrt[l]{b}$ is algebraic over K.

(b) If a is algebraic over K, then for all $n \in \mathbb{N}^+$ the element $\sqrt[n]{a}$ is algebraic over K as well.

112) Which of the following polynomials is primitive over $\mathbb{Z}_3$?

$$x^3 + x^2 + x + 1, \quad x^3 + x^2 + x + 2, \quad x^3 + 2x + 1.$$

113) Let K be a field with $\mathrm{char}(K) = p$. Prove that $(a + b)^p = a^p + b^p$ for all $a, b \in K$.

Hint: Use the binomial theorem and consider the equation $\binom{p}{k} = p \cdot \frac{(p-1)!}{k!(p-k)!}$ for $0 < k < p$. Show that $\binom{p}{k} \in \mathbb{N}$ implies that the fraction on the right-hand side must be an integer, too, since the factors in the denominator do not divide p.

114) Construct a field with 8 elements and demonstrate on some concrete examples how addition and multiplication are done in this field.

115) Consider the field $\mathbb{Z}_2[x]/(m(x))$ where $m(x) = x^8 + x^4 + x^3 + x + 1$. Hence the residue classes modulo $m(x)$ are

$$\overline{b(x)} = \overline{b_7x^7 + b_6x^6 + \cdots + b_1x + b_0}$$

and can be identified with a byte $b_7b_6 \cdots b_1b_0$. Compute the sum of the two bytes 10010101 and 11001100 in this field.

116) Show that the repetition code of order r (*i.e.* each bit of the original word is sent r times) is a linear code. Determine a generating matrix and a check matrix of this code.

117) Let

$$C = \{000000, 001011, 010101, 011110, 100110, 101101, 110011, 111000\} \subseteq \mathbb{Z}_2^6.$$

(a) Show that C is an (n, k) linear code and determine n and k.

(b) Determine a generating matrix and a check matrix of C.

(c) Determine the dual code $C^\perp$.

(d) Determine the cosets, their leaders and their syndromes.

(e) Use (d) to decode 010010 and 010110.

118) Four symbols have to be encoded with elements of $\mathbb{Z}_2^5$ such that the code forms a $(5, k)$ linear code (k to be determined) with which 1-bit errors can be detected and corrected. Determine a generating matrix and a check matrix of this code.

119) Examine if there is a cyclic code $C \subseteq \mathbb{Z}_2^6$ such that $001111 \in C$.

120) Let $p(x) = x^3 + 2$ be the generating polynomial of a cyclic $(9, 6)$ linear code over $\mathbb{Z}_3$. Determine a generating matrix such that this code is a systematic code, *i.e.* encoding is done by attaching one or more bits at the end of the original words.