MATH 504
EXERCISES 13

A. ZEYTİN

Unless otherwise stated R is a UFD.

(1) Let $p(X)$ be a polynomial in $K[X]$. Show that if $p(X)$ has a root in K, then $p(X)$ is reducible. Show by an example that the converse of this statement is false if the degree of is no less than 3.

(2) Decide whether the following polynomials are irreducible in the indicated rings. If no, find all irreducible factors :
- ▶ $p(X) = X^3 - 3X^2 + X - 3 \in \mathbf{R}[X]$
- ▶ $p(X) = X^3 - 3X^2 + X - 3 \in (\mathbf{Z}/5\mathbf{Z})[X]$
- ▶ $p(X) = X^4 + 1 \in \mathbf{R}[X]$
- ▶ $p(X) = X^4 + 1 \in \mathbf{Q}[X]$
- ▶ $p(X) = X^7 + 11X^3 - 33X + 22 \in \mathbf{Q}[X]$
- ▶ $p(X) = X^3 - 5 \in (\mathbf{Z}/5\mathbf{Z})[X]$
- ▶ $p(X) = X^3 - 5 \in (\mathbf{Z}/7\mathbf{Z})[X]$
- ▶ $p(X) = X^3 - 5 \in (\mathbf{Z}/11\mathbf{Z})[X]$
- ▶ $p(X) = X^3 - 7X^2 + 3X + 3 \in \mathbf{Q}[X]$
- ▶ $p(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbf{Q}[X]$
- ▶ $p(X) = X^3 - 2 \in \mathbf{Q}[X]$
- ▶ $p(X) = X^3 - 2 \in \mathbf{R}[X]$
- ▶ $p(X) = X^3 - 2 \in \mathbf{C}[X]$
- ▶ $p(X) = X^4 + X^2 + 2 \in (\mathbf{Z}/2\mathbf{Z})[X]$
- ▶ $p(X) = X^4 + X^2 + 2 \in (\mathbf{Z}/3\mathbf{Z})[X]$
- ▶ $p(X) = X^4 + X^2 + 2 \in (\mathbf{Z}/5\mathbf{Z})[X]$

(3) Decide whether the following rings are fields. If yes, determine their characteristic, write a basis as a vector space over $\mathbf{Z}/p\mathbf{Z}$ if $\mathrm{char}(K) = p$ and $\mathbf{Q}$ if $\mathrm{char}(K) = 0$:
- ▶ $R = \mathbf{Q}[X]/(X^2 + 1)$
- ▶ $R = \mathbf{C}[X]/(X^2 + 1)$
- ▶ $R = \mathbf{C}[X]/(X^2 + X + 1)$
- ▶ $R = (\mathbf{Z}/3\mathbf{Z})[X]/(X^4 + X + 1)$
- ▶ $R = \mathbf{Q}[X]/(X^9 + 3X^2 + 6)$
- ▶ $R = (\mathbf{Z}/5\mathbf{Z})[X]/(X^2 + X + 1)$
- ▶ $R = \mathbf{Q}[X]/(X^3 - 2)$

(4) Determine all the monic irreducible polynomials of degree 2 and 3 in the rings $(\mathbf{Z}/2\mathbf{Z})[X]$ and $(\mathbf{Z}/3\mathbf{Z})[X]$.

(5) Show that if $\varphi \colon K \to K'$ is a ring homomorphism between two fields then φ is necessarily injective. Deduce that K' must contain an isomorphic copy of K in such a case and hence can be viewed as an extension of K.

(6) Let K be a field and $p(X) \in K[X]$ be an irreducible polynomial of degree n.
- ▶ Verify that $L = K[X]/(p(X))$ is a field.
- ▶ Set $\alpha = X + (p(X))$. Show that $p(\alpha) = 0$ in $L[X]$, that is, the field L contains at least one root of $p(X)$.
- ▶ Show that the set $\mathcal{B} = \{1, \alpha, \ldots, \alpha^{n-1}\}$ is a K-linearly independent subset of L.
- ▶ Show that $\mathcal{B}$ is a basis of L as a vector space over K. Deduce that $[L : K] = n$.

(7) Show that extension degree is multiplicative : if L/K and M/L are two field extensions, then

$$[M : K] = [M : L][L : K]$$

.

(8) In this exercise, we are going to compare two fields with 8 elements:

- ► Show that the polynomials $p(X) = X^3 + X + 1$ and $q(X) = X^3 + X^2 + 1$ are irreducible over $(\mathbf{Z}/2\mathbf{Z})[X]$. Deduce that the rings $K_1 = (\mathbf{Z}/2\mathbf{Z})[X]/(p(X))$ and $K_2 = (\mathbf{Z}/2\mathbf{Z})[X]/(q(X))$ are fields with 8 elements.
- ► Write out the multiplication table of the groups $((\mathbf{Z}/2\mathbf{Z})[X]/(p(X)))^\times$ and $((\mathbf{Z}/2\mathbf{Z})[X]/(q(X)))^\times$.
- ► Show that K_1 and K_2 are isomorphic as fields.