MATH 511
EXERCISES 1

A. ZEYTİN

Throughout by K we denote a field and by R a commutative ring with identity.

(1) Let $p \in K[t]$ be a polynomial of degree $n \geq 1$ and let $R = K[t]/(p)$. Show that for and element $q \in R$ there is a unique polynomial $q_o \in R$ so that $\pi(p) = q_o$; where π denotes the canonical projection $\pi\colon K[t] \longrightarrow R$. What if $n = 0$?

(2) Let $p \in K[t]$. Show that the quotient $K[t]/(p)$ is a field if and only if p is irreducible.

(3) Apply Euclidean algorithm to the following polynomials, p and q, to find their greatest common divisor($\gcd$):
- ▶ $p(t) = t^3 - 1$ and $q(t) = t + 1 \in \mathbf{Q}[t]$
- ▶ $p(t) = t^3 + 4t^2 + t - 6$ and $q(t) = t^5 - 6t + 5$ in $\mathbf{Q}[t]$

In each case, write $\gcd$ as a linear combination of p and q.

(4) Show that
- ▶ units in a ring R form a group.
- ▶ for I and J ideals of R so that $I + J = R$, there is a isomorphism between the unit groups of the rings $R/(I \cap J)$ and $R/I \oplus R/J$.

Write and prove an appropriate generalization of this theorem and explain why this is a generalization of Chinese Remainder Theorem.

(5) Show that if $p(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ has a root in $\mathbf{Q}$ then it has a root, say $m \in \mathbf{Z}$. In this case, show that $m | a_0$.

(6) Decide whether the following polynomials are irreducible over the given rings
- ▶ $p(t) = t^4 + 4$ over $\mathbf{Z}/5\mathbf{Z}$
- ▶ $p(t) = t^3 + 2t^2 + 2t + 1$ over $\mathbf{Z}/7\mathbf{Z}$
- ▶ $p(t) = t^3 + 3t^2 - 8$ over (use previous exercise.)
- ▶ $p(t) = t^4 - 22t^2 + 1$ over $\mathbf{Z}[t]$
- ▶ $p(t) = 8t^3 + 6t^2 - 9t + 24$ over $\mathbf{Z}[t]$
- ▶ $p(t) = 2t^{10} - 25t^3 + 10t^2 - 30$ over $\mathbf{Z}[t]$

(7) Show that extension degree of fields is multiplicative, i.e if L is a finite extension of K and K is a finite extension of F then:

$$[L : F] = [L : K][K : F].$$

(8) Determine the ring of integers of quadratic number fields, i.e $\mathbf{Q}(\sqrt{d})$; where d is a square-free integer.

(9) Show that an element α of a ring of integers $\mathcal{O}_K$ is a unit if and only if its norm over $\mathbf{Q}$ is ± 1. Show that $x + y\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$ is a unit if and only if the pair (x, y) is a solution to either the Pell equation $x^2 - dy^2 = 1$ or the equation $x^2 - dy^2 = -1$.

(10) Recall that an integral domain R is said to be a *Euclidean domain* if there exists a norm map $N : R \longrightarrow \mathbf{N} \cup \{0\}$ satisfying:
- i. $N(r) = 0$ if and only if $r = 0$,
- ii. For all $a, b \in R$, with b non-zero, there exist $q, r \in R$ such that $a = bq + r$, and $N(r) < N(b)$.
- ▶ Show that a Euclidean domain is a principal ideal domain, and deduce that it is a unique factorization domain.
- ▶ Show that $\mathbf{Z}[\sqrt{d}]$ is a Euclidean domain if $d = -2, -1, 2 or 3$.

(11) Show that for $K = \mathbf{Q}(\sqrt[3]{2}$, the norm of the element $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, we have $N_K(\alpha) = a^3 + 2b^3 + 4c^3 - 6abc$. Try to obtain a similar formula for the trace.

(12) Let $\zeta_5 = e^{2\pi\sqrt{-1}/5}$ and consider the field $K = \mathbf{Q}(\zeta_5)$.

- ▶ Find the minimal polynomial of ζ_5.
- ▶ Determine all the embeddings of K into $\mathbf{C}$.
- ▶ For an element $\alpha = a + b\zeta_5 \in \mathbf{Q}(\zeta_5)$ prove that $N_K(\alpha) = \frac{a^5+b^5}{a+b}$. Using this, compute $N_K(1+\zeta_5)$.