# MATH 468
# EXERCISE SET 1

A. ZEYTİN

(1) The aim of this exercise is to get you familiar with the field of fractions of an integral domain, $R$. Define the set

$$Q_o(R) := \{(a,b) | a, b \in R, b \neq 0\}.$$

Define two elements $(a,b)$ and $(a',b')$ to be equivalent and write $(a,b) \sim (a',b')$, if $ab' - a'b = 0$.

i. Show that $\sim$ is an equivalence relation, i.e. it is reflexive, symmetric and transitive.

Let $Q(R)$ be the set of equivalence classes under this equivalence relation. Denote the class of a pair $(a,b)$ by $[a,b]$. Define the following two operations of $Q(R)$:

$$[a,b] + [c,d] = [ad + bc, bd] \text{ and } [a,b] \cdot [c,d] = [ac, bd].$$

ii. Show that addition and multiplication are well defined, i.e. they are independent of the chosen representative.

iii. Show that with the above operations $Q(R)$ becomes a field.

iv. Prove that the map

$$\iota : R \longrightarrow Q(R)$$

defined as $\iota(r) = [r, 1]$ is an injective ring homomorphism(or a monomorphism).

Note: If you feel uncomfortable with general fields, try to imagine what's going on in case $R = \mathbf{Z}$. What is $Q(\mathbf{Z})$?

(2) Let $\mathbf{Z}[\sqrt{-1}] := \{a + b\sqrt{-1} \in \mathbf{C} \mid a, b \in \mathbf{Z}\}$.

i. Show that $\mathbf{Z}[\sqrt{-1}]$ is an integral domain.

ii. Repeat Exercise 1 for $\mathbf{Z}[\sqrt{-1}]$. What is $Q(\mathbf{Z}[\sqrt{-1}])$?

(3) Let $k$ be a field. Prove that if $f(X) \in k[x]$ is a polynomial of degree 2 or 3 then $f(x)$ is irreducible in $k[x]$ if and only if $f(x)$ has no root in $k$.

(4) Find the **monic**, single generator of the following ideals:

i. $I = (x^2 - 7, x^2 + 7)$ in $\mathbf{Q}[x]$

ii. $I = (x^6 - 8, x^2 - 2)$ in $\mathbf{Q}[x]$

iii. $I = (x^3 + 4x^2 + x - 6, x^5 - 6x + 5)$ in $\mathbf{Q}[x]$

Hint: Modify the Euclidean algorithm to the case of polynomials.

Note: In case you need, look up the definition of an ideal generated by two elements.

(5) Prove that $(x)$ and $(x, y)$ are both prime ideals in $\mathbf{Q}[x, y]$, i.e. polynomials in two variable, $x$ and $y$. Show also that only the ideal $(x, y)$ is maximal.

Hint: Consider the quotient rings!

(6) For a prime number $p$ define $\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{p-1}$. This polynomial is called the $p^{th}$ cyclotomic polynomial. Show that $\Phi_p(x) \in \mathbf{Q}[x]$ is irreducible using the Eisenstein criterion.

Hint: A change of variable $x \mapsto x + 1$ might help.

(7) Determine whether the following polynomials are irreducible over the given polynomial rings:

i. $x^2 + x + 1$ over $\mathbb{F}_2[x]$

ii. $x^3 + x + 1$ over $\mathbb{F}_3[x]$

iii. $x^4 + 1$ over $\mathbb{F}_5[x]$

iv. $\frac{(x+2)^p - 2^p}{x}$ over $\mathbf{Q}[x]$; where $p$ is an odd prime.

v. $x^4 + 4x^3 + 6x^2 + 2x + 1$ over $\mathbf{Q}[x]$ Hint: In this case, use $x \mapsto x - 1$

(8) Construct a field with 27 elements.

Hint: Try to find an irreducible polynomial of degree 3 over $\mathbb{F}_3$.

(9) Construct a field with 25 elements.

(10) Find the minimal polynomial of $\alpha = \sqrt[6]{2}$ over $\mathbf{Q}$. What is the minimal polynomial of $\alpha$ over $\mathbf{Q}(\sqrt{2})$?

(11) Let $p$ and $q$ be two **distinct** prime numbers.

i. What is the minimal polynomial of $\sqrt{p}$ over $\mathbf{Q}$?

ii. What is the minimal polynomial of $\sqrt{q}$ over $\mathbf{Q}(p)$?

iii. What is the degree of the extension $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$?

iv. Find a basis for the vector space $\mathbf{Q}(\sqrt{p}, \sqrt{q})$ over $\mathbf{Q}$.