Content of a polynomial in $\mathbb{Q}[X]$. The ring $\mathbb{Z}[X]$

Problem 1. Let A be a commutative unitary ring. We consider the ring $A[X]$ of polynomials with coefficients in A.

(1) Identify $(A[X])^{\times}$.

(2) Show that $A[X]$ is an integral domain if and only if A is an integral domain.

(3) Now we suppose that $A = \mathbb{Z}$. A polynomial P in $\mathbb{Z}[X]$ is called primitive if the only elements of $\mathbb{Z}$ that divide all coefficients of P at once are ± 1. A polynomial P in $\mathbb{Z}[X]$ is called irreducible if $P = AB$ where $A, B \in \mathbb{Z}[X]$ implies that A or B is a unit of $\mathbb{Z}[X]$.

  (a) Show that $\mathbb{Z}[X]$ is not principal.

  (b) Show that the product of two primitive polynomials in $\mathbb{Z}[X]$ is primitive.

  (c) Show that a nonzero polynomial $Q \in \mathbb{Q}[X]$ can be written uniquely in the form $Q = c(Q)P$ with $P \in \mathbb{Z}[X]$ primitive and $c(Q) \in \mathbb{Q}$, $c(Q) > 0$. Check that $c(Q) \in \mathbb{Z}$ if and only if $Q \in \mathbb{Z}[X]$. The rational number $c(Q)$ is called the content of Q.

  (d) Show that for $A, B \in \mathbb{Q}[X]$ we have $c(A)c(B) = c(AB)$.

  (e) Prove the following statement

  Lemma (Gauss Lemma)**.** *A non constant polynomial $P \in \mathbb{Z}[X]$ is irreducible if and only if it is primitive and irreducible when seen as a polynomial in $\mathbb{Q}[X]$.*

  (f) Prove Eisenstein's criterion (cf HW2).

Problem 2. (1) Let $g \in \mathbb{Z}[X]$ be a non constant polynomial. We are going to show that $\mathbb{Z}[X]/g\mathbb{Z}[X]$ is not a field.

  (a) What is the characteristic of the ring $\mathbb{Z}[X]/g\mathbb{Z}[X]$?

  (b) Show that there is $a \in \mathbb{Z}$ such that $g(a) \neq 0, \pm 1$ and let p be a prime number dividing $g(a)$.

  (c) Show that there is a unique well defined surjective morphism of rings

$$\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}$$

  sending X onto $a \bmod p$ and that it factors through $\mathbb{Z}[X]/g\mathbb{Z}[X]$. Show that the resulting map $\varphi : \mathbb{Z}[X]/g\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}$ is not injective.

  (d) Conclude.

(2) Let $f \in \mathbb{Z}[X]$ primitive. Show that $[f\mathbb{Q}[X]] \cap \mathbb{Z}[X] = f\mathbb{Z}[X]$.

(3) Let $\mathfrak{I}$ be a maximal ideal of $\mathbb{Z}[X]$ and $k := \mathbb{Z}[X]/\mathfrak{I}$. Suppose that $\mathbb{Z} \cap \mathfrak{I} = \{0\}$.

(a) Show that the ideal of $\mathbb{Q}[X]$ generated by $\mathfrak{I}$ is a proper ideal and denote by g a generator. Check that one can choose $g \in \mathbb{Z}[X]$ primitive. Check that $\mathfrak{I}$ is contained in $g\mathbb{Z}[X]$.

(b) Show that the natural projection $\mathbb{Z}[X] \to \mathbb{Z}[X]/g\mathbb{Z}[X]$ induces an isomorphism of rings $k \simeq \mathbb{Z}[X]/g\mathbb{Z}[X]$.

(c) Conclude.

(4) Prove that the maximal ideals of $\mathbb{Z}[X]$ are the ideals of the form $< p, f >$ where p is a prime number and $f \in \mathbb{Z}[X]$ is such that its projection $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ is irreducible.