Exercise Sheet 2

Exercise 1
A polynomial $f(X) \in \mathbb{Z}[X]$ is primitive if the greatest common divisor of its coefficients is 1. Show the following:

1. If $f(X), g(X) \in \mathbb{Z}[X]$ are primitive, then the product $f(X)g(X)$ is also primitive.
2. $f(X) \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ if and only if it is primitive and irreducible in $\mathbb{Q}[X]$.
3. If a monic $f(X) \in \mathbb{Z}[X]$ factors as $f(X) = g(X)h(X)$ with $g(X), h(X) \in \mathbb{Q}[X]$ monic, then $g(X), h(X) \in \mathbb{Z}[X]$.

Do the analogous statements hold if we replace $\mathbb{Z}$ by any UFD A, and $\mathbb{Q}$ by its field of fractions $K = \mathrm{Quot}(A)$.

Solution
<u>1.</u>
Denote the coefficients of f and g with a_i and b_j for $1 \leq i \leq \deg f$ and $1 \leq j \leq \deg g$ such that

$$f(X) = \sum_{i=0}^{\deg f} a_i X^i \qquad\qquad g(X) = \sum_{j=0}^{\deg g} b_j X^j \tag{1}$$

Assume there is a prime $p \in \mathbb{Z}$ that divides all coefficients of fg and let a_n and b_m be the first coefficients in f and g respectively that are not divisble by p. Such a_n and b_m must exist because f and g are primitive.

Consider X^{n+m} in the polynomial fg. The coefficient for this term is the sum of products of a_i and b_j for which $i + j = n + m$, i.e.

$$a_n b_m + a_{n-1} b_{m+1} + a_{n+1} b_{m-1} + a_{n-2} b_{m+2} + \dots . \tag{2}$$

This coefficient is however not divisible by p as p divides all but the first term. Hence we have a contradiction.
<u>2.</u>
Let f be irreducible in $\mathbb{Z}[X]$ and assume that is reducible in $\mathbb{Q}[X]$. From the assumption, we have that $f(X) = g(X)h(X)$ for some $g, h \in \mathbb{Q}[X]$ that are not units in $\mathbb{Q}[X]$.

For two rational numbers, the greatest common divisor is defined as in the following manner

$$\gcd\left(\frac{a}{b}, \frac{c}{d}\right) = \frac{\gcd(a \cdot d, b \cdot c)}{b \cdot d}. \tag{3}$$

We also have

$$\left(\frac{b \cdot d}{\gcd(a \cdot d, b \cdot c)}\right) \cdot \left(\frac{a}{b}\right) = \frac{a \cdot d}{\gcd(a \cdot d, b \cdot c)} \in \mathbb{Z}. \tag{4}$$

as $\gcd(a \cdot d, b \cdot c)$ divides a or d.

Define d_g and d_h to be the greatest common divisor of the coefficients of g and h respectively. Consider $\tilde{g} := d_g^{-1} g$ and $\tilde{h} := d_h^{-1} h$. From above, we know that $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$, and moreover, these are primitive. Hence their product

$$\tilde{g}\tilde{h} = d_g^{-1} d_h^{-1} gh = d_g^{-1} d_h^{-1} f \tag{5}$$

is also primitive.

But f is also already primitive and since $\tilde{g}\tilde{h} \in \mathbb{Z}[X]$ we have that $d_g^{-1}d_h^{-1} = 1$. In other words, we have a factorization $f(X) = \tilde{g}(X)\tilde{h}(X)$ which is a contradiction.

On the other hand, let f be primitive and irreducible in $\mathbb{Q}[X]$, but assume it is reducible in $\mathbb{Z}[X]$.

If f is a constant, then it is $f(X) = \pm 1$ as f is primitive. This is a contradiction, however, because ± 1 is a unit in $\mathbb{Q}[X]$.

Consider the case where $\deg \geq 1$. From the assumption, we have a factorization $f(X) = g(X)h(x)$ with $g, h \in \mathbb{Z}[X]$ but $g, h \neq \pm 1$.

Assume g is a constant, then g divides all coefficient of f in $\mathbb{Z}$. This cannot be since f is primitive. Therefore, we have $\deg g \geq 1$ which means that g is not a unit in $\mathbb{Q}[X]$.

Apply the same argument for h and we have $f(X) = g(X)h(X)$ is a non-trivial factorization in $\mathbb{Q}[X]$. This is a contradiction with the first assumption.

3.
Let $f \in \mathbb{Z}[X]$ be monic and $f(X) = g(X)h(X)$ with g and h monic. Assume $g, h \notin \mathbb{Z}[X]$. There are some $n \in \mathbb{Z}$ such that $nf(X) = \tilde{g}(X)\tilde{h}(X)$ such that $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$ (e.g. least common multiple) and let n be the smallest of such integers.

Since from the assumption we know that $n \geq 1$, there is a $p \in \mathbb{Z}$ that divides n. Now assume p does not divide all coefficients of $\tilde{g}$ nor $\tilde{h}$. Similary to 1., let a_n and b_m be the first coefficients that are not divisble by p and consider the coefficient for X^{n+m}. We again have

$$a_n b_m + a_{n-1}b_{m+1} + a_{n+1}b_{m-1} + a_{n-2}b_{m+2} + \dots \tag{6}$$

which is not divisble by p. Therefore, p must divide $\tilde{g}$ or $\tilde{h}$. We have

$$\frac{n}{p} f(X) = \hat{g}\hat{h} \tag{7}$$

with $\hat{g}, \hat{h} \in \mathbb{Z}[X]$. This is a contradiction however, as we required n to be the smallest integer.

All three proofs can be analogously applied to any UFD A and $\mathrm{Quot}(A)$.