Rings and Fields
Assignment 5

James Zoryk.
Student Number: 2663347.

Question 1. Factorise the following polynomials into irreducible factors in the given Unique Factorisation Domains.

Part A. $5x^7 + 10$ in $\mathbb{Q}[x], \mathbb{Z}[x]$

Proof. Consider $f(x) = 5x^7 + 10$ in $\mathbb{Z}[x]$. Now consider the map: $\psi(\mathbb{Z}[x]) \to \mathbb{Z}[x]$, define as $\psi(f(x)) \mapsto f(y+1)$ which is a ring isomorphism to itself, since an inverse map exists $\psi^{-1}(f(\hat{x}+1)) \mapsto f(x)$. If we assume that $f(x)$ is reducible, then $f(x) = g(x)h(x)$ for some polynomial factors $g(x), h(x)$ in $\mathbb{Z}[x]$ with lower degree than $f(x)$. Then applying the map we have, $f(\hat{x}+1) = g(\hat{x}+1)h(\hat{x}+1)$, thus reducible of $f(x)$ implies $f(\hat{x}+1)$ is reducible over $\mathbb{Z}[x]$. The contrapositive, if $f(x)$ is irreducible in $\mathbb{Z}[x]$ then $f(\hat{x}+1)$ is also irreducible in $\mathbb{Z}[x]$, is also true.
Now applying $\psi(f(x))$, we have

$$f(\hat{x}+1) = 5\hat{x}^7 + 35\hat{x}^6 + 105\hat{x}^5 + 175\hat{x}^4 + 175\hat{x}^3 + 105\hat{x}^2 + 35\hat{x} + 15 \in \mathbb{Z}[x].$$

Choosing $p = 7$, which is prime in $\mathbb{Z}$, we observe that $7|35, 105, 175$ and that $7 \not| \ 5$, $7^2 \not| 15$. By Eisensetien's Criterion $f(\hat{x}+1)$ is an irreducible polynomial in $\mathbb{Q}[x]$
Moreover, applying $\phi^{-1}(f(\hat{x}+1))$ we can deduce that $f(x)$ is in fact irreducible in $\mathbb{Q}[x]$ and thus can not be Factorised in $\mathbb{Q}[x]$. $\square$

Part B. $5x^7 + 10$ in $\mathbb{Z}[x]$

Proof. Let $f(x) = 5x^7 + 10$ in $\mathbb{Z}[x]$, then it can be factorised $f(x) = (5)(x^7 + 2)$, where 5 is not a unit in the integral domain $\mathbb{Z}[x]$, and since 5 is prime in $\mathbb{Z}$ it is irreducible. However we need to show that $g(x) = (x^7+2)$ is irreducible in $\mathbb{Z}[x]$. Once again consider the map ψ define in section A, then it follows that $\psi(g(x))$ is equal to

$$f(\hat{x}+1) = \hat{x}^7 + 7\hat{x}^6 + 21\hat{x}^5 + 35\hat{x}^4 + 35\hat{x}^3 + 21\hat{x}^2 + 7\hat{x} + 3 \in \mathbb{Z}[x].$$

Choosing $p = 7$, which is prime in $\mathbb{Z}$, $7|35, 21, 7$ and $7 \not| 1$ with $7^2 \not| 3$. By Eisensetien's Criterion $g(\hat{x}+1)$ is an irreducible polynomial in $Frac(\mathbb{Z})[x]$. As the polynomial $g(\hat{x}+1)$ is monic it is irreducible in $\mathbb{Z}[x]$, by Gauss's lemma.
Since ψ is a bijection, we can conclude that $g(x)$ is irreducible in $\mathbb{Z}[x]$. Thus $f(x) = (5)(x^7 + 2)$ in $\mathbb{Z}[x]$. $\square$

Part C. $x^4 + 5x^3 + 1$ in $\mathbb{Q}[x]$

Proof. Suppose that $f(x) = x^4 + 5x^3 + 1$ is reducible in $\mathbb{Z}_2[x]$, then it factors in $\mathbb{Z}_2[x]$, so it must therefore either have a linear factor in $\mathbb{Z}_2[x]$ or factors into two quadratics in $\mathbb{Z}_2[x]$.
The only possibilities for a linear factor in $\mathbb{Z}_2[x]$ are 0 and 1, which will be root of $f(x) = 0$, but we see that $f(0) = 1$ and $f(1) = 1$, neither of which are roots of the polynomial in $\mathbb{Z}_2[x]$. We can conclude that $f(x)$ in $\mathbb{Z}_2[x]$ has no linear factor.
Now, lets consider that $f(x)$ factors into a product of two quadratic polynomials in $\mathbb{Z}_2[x]$. However, the only irreducible quadratic polynomial in $\mathbb{Z}_2[x]$ is $g(x) = x^2 + x + 1$. Note that $x^2 = (x)(x)$, $x^2 + x = x(x + 1)$ and $x^2 + 1 = (x + 1)(x + 1)$. We observe that the square of $g(x)$ in $\mathbb{Z}_2[x]$ is $x^4 + x^2 + 1 \neq f(x)$. We arrive at contradiction, hence $f(x)$ is an irreducible in $\mathbb{Z}_2[x]$.
Since 2 is prime in $\mathbb{Z}$, $f(x)$ is monic polynomial and a irreducible in $\mathbb{Z}_2[x]$, it implies that $f(x)$ in $\mathbb{Z}[x]$ will be irreducible over $\mathbb{Z}$.
As $\mathbb{Z}[x]$ is a Unique Factorisation Domain, $f(x)$ is monic polynomial and irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $Q[x]$.

□

Part D. $yx^5 + (2y^4 + 4y)x + 2y^2 + 2y$ in $\mathbb{Z}[x, y]$

Proof. Let $f(x, y) = yx^5 + (2y^4 + 4y)x + 2y^2 + 2y$ in $\mathbb{Z}[x, y]$, then there exist a canonical isomorphism $\mathbb{Z}[x, y] \cong \mathbb{Z}[y][x]$, such that $f(x)$ is in $\mathbb{Z}[x]$ with it's coefficients in $\mathbb{Z}[y]$.
Observe that $f(x, y) = (y)(x^5 + x(4 + y^3) + (2 + 2y))$, with (y) being an irreducible as the degree of the polynomial is 1. We need to check if $g(x, y) = x^5 + x(4 + y^3) + (2 + 2y)$ is irreducible in $\mathbb{Z}[y][x]$. We want to show that $2y^3 + 4$ and $2y + 2$ is divisible by some prime ideal p in $\mathbb{Z}[y]$, with the conditions that p does not divide y, and p^2 does not divide $2y^2 + 2y$.
Now, consider $p = (2)$. The ideal (2) is prime in the coefficients ring $\mathbb{Z}[y]$, since $\mathbb{Z}[y]/(2) = \mathbb{Z}_2[y]$ is an integral domain as it is a subring of the integral domain $\mathbb{Z}[y]$.
So indeed we can applying the Eisensetien's Criterion to $g(x, y)$ with $p = 2$, as $2 | 2y^3 + 4, 2y + 2$, $2 \not| y$ and $2^2 \not| 2y + 2$, so that $g(x, y)$ is irreducible in $Frac(\mathbb{Z}[y])[x]$. As the GCD of the coefficients of $g(x, y)$ is 1, a unit in $Frac(\mathbb{Z}[y])[x]$, we can conclude that $g(x, y)$ is irreducible in $\mathbb{Z}[x, y]$.

□