Fields, rings, and modules
Exercise sheet 2

https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22102/index.html

Version: March 9, 2020

Answers are due for Thursday March 12th, 4PM.

Exercise 1 *Factorisation of polynomials (100 pts)*

Justify your answers carefully in order to receive full credit.

1. (8 pts) Let K be a field, and let $F(x) \in K[x]$ of degree 1. Prove that $F(x)$ is irreducible in $K[x]$.

   Hint: What could be the degrees of the factors?

2. (7 pts) Give an example of a ring R and of a polynomial $F(x) \in R[x]$ of degree 1 such that $F(x)$ is not irreducible in $R[x]$.

3. (15 pts) Let K be a field, and let $F(x) \in K[x]$ of degree 2 or 3. Prove that $F(x)$ is reducible in $K[x]$ if and only if it has a root in K.

   Hint: What could be the degrees of the factors?

4. (10 pts) Give an example of a polynomial in $\mathbb{R}[x]$ which is reducible in $\mathbb{R}[x]$ but has no root in $\mathbb{R}$.

5. (15 pts) Let $F(x) \in \mathbb{Z}[x]$ be non-constant and monic, and let $n \geqslant 2$ be an integer. Prove that if $F(x)$ is irreducible in $(\mathbb{Z}/n\mathbb{Z})[x]$, then $F(x)$ is irreducible in $\mathbb{Z}[x]$.

   Hint: Proceed by contradiction.

6. (15 pts) Prove that $F(x) = x^3 + x + 1$ in irreducible in $\mathbb{Z}[x]$ **and** in $\mathbb{Q}[x]$.

   Hint: Reduce mod 2 and use the previous questions.

7. (10 pts) Prove that $F(x) = x^5 + 4x + 2$ in irreducible in $\mathbb{Z}[x]$ **and** in $\mathbb{Q}[x]$.

8. (20 pts) Prove that $F(x, y) = x^5 - x^3y + xy^7 + 2y$ is irreducible in $\mathbb{C}[x, y]$.

Solution 1

1. Suppose $F(x) = G(x)H(x)$ with $G, H \in K[x]$. Since K is a field, it is a domain, so we have
$$1 = \deg F = \deg G + \deg H.$$
Since obviously G and H cannot be 0 (for else $F = GH$ would be 0), they have non-negative degrees, so we must have $\deg G = 1$ and $\deg H = 0$ or vice versa. Suppose without loss of generality that $\deg G = 1$ and $\deg H = 0$. Then H is a nonzero constant, so it is invertible in K since K is a field, and hence in $K[x]$. Therefore, we have proved that any factorisation of F in $K[x]$ involves a unit and an associate to F, which means that F is irreducible.

2. By the previous question, we must choose R so that it is not a field. We can take $R = \mathbb{Z}$, and $F(x) = 2x$. Since $\mathbb{Z}$ is a domain, we have
$$\mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{\pm 1\},$$
so neither 2 nor x are invertible in $\mathbb{Z}[x]$; thus $F(x)$ is not irreducible in $\mathbb{Z}[x]$.

   Remark: In fact, both 2 and x are irreducible in $\mathbb{Z}[x]$, since $\mathbb{Z}$ is a UFD, and since the former is constant and irreducible in $\mathbb{Z}$, and the latter is irreducible in $\mathbb{Q}[x]$ by the previous question. So $F(x) = 2 \cdot x$ is the complete factorisation of F in $\mathbb{Z}[x]$.

3. Since K is a field, it is a domain, so for all $a \in K$, we have
$$F(a) = 0 \iff (x - a) \mid F(x).$$
So if $F(x)$ has a root, say a, then it has $x - a$ as a factor. This factor has degree 1, and since K is a domain we deduce that the cofactor has degree $\deg F - \deg(x - a) = \deg F - 1 > 0$. Since K is a domain, $K[x]^\times = K^\times$, so neither factor is invertible, so $F(x)$ is not irreducible.

   Remark: This implication F has root $\Rightarrow$ F is reducible works even in any degree, except in degree 1 of course.

   Conversely, suppose is reducible in $K[x]$. Then $F = GH$ with $G, H \in K[x]$ non-units, i.e. non-constant so of positive degree. As $\deg G + \deg H = \deg F \leqslant 3$, one of the factors, say G, has degree 1. Then $G(x) = ax + b$ with $a, b \in K$, $a \neq 0$. Since K is a field, a is invertible, and $-b/a \in K$ is a root of G, and thus of $F = GH$. So F has at least one root in K.

4. By the above, we want a polynomial without roots in $\mathbb{R}$ and of degree at least 4. If one of the factors has degree 1, then we have a root, so we must avoid that too. So we can take a product of two irreducibles of degree 2 (or more), since then neither will have a root by the previous question, so their product won't have a root either since $\mathbb{R}$ is a domain (In fact, by the previous question, the fact that our factors have no roots will ensure that they are irreducible, as long as their degrees does not exceed 3). More specifically, we can take
$$(x^2 + 1)(x^2 + 2) \in \mathbb{R}[x]$$
or even
$$(x^2 + 1)^2 \in \mathbb{R}[x].$$

Remark: These polynomials have roots in $\mathbb{C}$, and thus become reducible in $\mathbb{C}[x]$.

5. Suppose by contradiction that F is reducible in $\mathbb{Z}[x]$, say $F = GH$ with $G, H \in \mathbb{Z}[x] \setminus \mathbb{Z}[x]^\times$. Let g (resp. h) be the leading coefficient of G (resp. H); then $g, h \in \mathbb{Z}$ and $gh =$ leading coefficient of $F = 1$, so $g = h = \pm 1$. Replacing G and H by their negatives if needed, we may assume that G and H are monic. Besides, they are non-constant, for else thy would be invertible in $\mathbb{Z}[x]$. Thus in $(\mathbb{Z}/n\mathbb{Z})[x]$ we have $\bar{F} = \bar{G}\bar{H}$.

   We want to conclude that $\bar{F}$ is reducible in $(\mathbb{Z}/n\mathbb{Z})[x]$. For this, we must show that neither $\bar{G}$ nor $\bar{H}$ are invertible there. Suppose for instance that $\bar{H}$ is invertible, say $\bar{H}\bar{K} = \bar{1}$ for some $\bar{K} \in (\mathbb{Z}/n\mathbb{Z})[x]$. Then we can write

$$\bar{H} = x^m + \text{ lower terms},$$

$$\bar{K} = \bar{a}x^n + \text{ lower terms},$$

   where $m > 0$ and $a \neq 0$, so that

$$\bar{1} = \bar{H}\bar{K} = \bar{a}x^{m+n} + \text{ lower terms}$$

   which is a contradiction since $m + n \geqslant m > 0$.

6. Let us first prove that F is irreducible in $\mathbb{Z}[x]$ by applying the previous question with $n = 2$. Let $\bar{F} = x^3 + x + \bar{1} \in (\mathbb{Z}/2\mathbb{Z})[x]$. Since 2 is a prime number, $\mathbb{Z}/2\mathbb{Z}$ is a field, so question 3. tells us that $\bar{F}$ is irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$ iff. it has no roots in $\mathbb{Z}/2\mathbb{Z}$. But the only elements of $\mathbb{Z}/2\mathbb{Z}$ are $\bar{0}$ an $\bar{1}$, so that's only 2 potential roots. Since

$$\bar{F}(\bar{0}) = \bar{1} \neq \bar{0}$$

   and

$$\bar{F}(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$$

   we conclude that $\bar{F}$ has no roots in $\mathbb{Z}/2\mathbb{Z}$ and is thus irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$.

   By the previous question, F is irreducible in $\mathbb{Z}[x]$.

   Since $\mathbb{Z}$ is a UFD, the irreducibles in $\mathbb{Z}[x]$ ar irreducible constants and primitive polynomials that are irreducible in $\mathbb{Q}[x]$. Clear F does not fall into the first category, so it must fall into the second one. This shows that F is irreducible over $\mathbb{Q}$.

7. $\mathbb{Z}$ is a UFD, $p = 2$ is irreducible in $\mathbb{Z}$, and F is Eisenstein at 2 since $2 \mid 0, 4, 2$ in $\mathbb{Z}$ and $2^2 \nmid 2$ in $\mathbb{Z}$. Therefore F is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

8. Since $\mathbb{C}$ is a field, $\mathbb{C}[y]$ is a ED, hence a PID, hence a UFD. Besides y is irreducible in $\mathbb{C}[y]$ by question 1. Finally, $F \in \mathbb{C}[x, y] = \mathbb{C}[y][x]$ is Eisenstein at y since $y \mid 0, -y, y^7, 2y$ in $\mathbb{C}[y]$ and $y^2 \nmid 2y$ in $\mathbb{C}[y]$. Therefore F is irreducible in $\mathbb{C}[y][x] = \mathbb{C}[x, y]$ (and also in $(\operatorname{Frac}\mathbb{C}[y])[x] = \mathbb{C}(y)[x]$).