# Algebra II: Tutorial 2

February 21, 2022

**Problem 1.** Let $R$ be an integral domain. Show that if $R[x]$ is a UFD, then $R$ is again a UFD.

**Solution.** Consider any non-unit element $a$ in $R$ as an element of degree zero in $R[x]$. Since $R[x]$ is a UFD, $a$ has a unique factorisation into irreducibles in $R[x]$. By the additive property of degrees, each irreducible component has degree zero. We know that irreducibles in $R[x]$ of degree zero are in bijection with irreducibles in $R$. This concludes our proof. ∎

**Problem 2** (Relation between irreducibility and existence of roots)**.** Let $K$ be any field, and consider the polynomial ring $R = K[x]$.

1. Suppose that $f \in R$ has degree 2 or 3. Show that $f$ is irreducible over $K$ if and only if $f$ has no roots in $K$.

2. Show that the statement in part 1. no longer holds if we assume that $f$ has degree $\geq 4$.

3. Show that the statement in part 1. is no longer true if we replace $K$ by an arbitrary integral domain.

**Solution.** 1. Suppose that $f$ is reducible. Since $f$ has degree 2 or 3, the additive property of degrees implies that $f$ must have a linear factor, in which case $f$ has a root. The converse is true without the assumption on the degree of $f$.
2. The polynomial $(x^2+2)^2$ is reducible over $\mathbb{Q}$ yet does not have roots in $\mathbb{Q}$.
3. Consider $f = 2x^{+}4$ over $\mathbb{Z}$. Then, $f$ is reducible and has degree two, but has no roots in $\mathbb{Z}$.

**Problem 3** (Irreducibility tests over $\mathbb{Q}$)**.** Determine whether or not the following polynomials are irreducible over $\mathbb{Q}$:

1. $f(x) = x^3 + 5x^2 + 4$,

2. $f(x) = x^4 - 10x^2 + 1$.

**Solution.** 1. Since $f$ is primitive, $f$ is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$. To show that $f$ is irreducible over $\mathbb{Z}$, note that over $\mathbb{Z}_3$, $f(x) = x^3 + 2x^2 + 1$ has no roots. This implies that $f$ is irreducible over $\mathbb{Z}_3$, which by the mod$-p$ lemma, implies $f$ is irreducible over $\mathbb{Z}$.
2. By Gauss's lemma, it suffices to show that $f(x)$ is irreducible over $\mathbb{Z}$. Suppose that $f$ is reducible over $\mathbb{Z}$. A direct computation using the root test shows that $f$ has no root in $\mathbb{Z}$. Therefore, $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ for some $a, b, c, d \in \mathbb{Z}$. A quick calculation shows this is not possible, and hence such a factorisation does not exist. ■

**Problem 4** (Universal property of polynomial rings)**.** Let $K$ be a commutative ring, and $L$ a ring containing $K$ as a subring. Consider the polynomial ring $K[x]$.

1. For each $\alpha \in L$, show that there exists a unique ring homomorphism

$$ev_\alpha : K[x] \to L,$$

   satisfying the following two conditions:

   (a) $ev_\alpha(k) = k$, for all $k \in K$, and

   (b) $ev_\alpha(x) = \alpha$.

   For each $\alpha \in L$, we call that homomorphism the *evaluation homomorphism at* $\alpha$.

2. Suppose now that $K$ is an infinite field, and $L = K$. Show that $f \in K[x]$ and $g \in K[x]$ are equal if and only if the evaluations $ev_\alpha(f)$ and $ev_\alpha(g)$ are equal in $K$ for *all* elements $\alpha \in K$.

3. Show that this property does not hold if $K$ is a finite field. (Hint: find two distinct polynomials $f$ and $g$ over $\mathbb{Z}_3$ whose values $f(\alpha)$ and $g(\alpha)$ coincide $\forall \alpha \in \mathbb{Z}_3$.)

**Solution.** 1. For $f(x) = \sum_{n=0}^{m} a_n x^n$ with $a_n \in K \subset L$, define $\phi_a(f(x)) = \sum_{n=0}^{m} a_n \alpha^n$. Since $K$ is a subring of $L$, the image of $ev_\alpha$ lies in $L$. It is easy to see that $ev_\alpha(k) = k$ for all $k \in K$, and that $ev_\alpha(x) = \alpha$. It is straightforward to see that $ev_\alpha$ is a ring homomorphism. Suppose now that $\phi_1$ and $\phi_2$ are two such ring homomorphisms from $K[x]$ to $L$, i.e. ring homomorphisms fixing $K$ and such that $\phi_1(x) = \phi_2(x) = \alpha$. Since $\phi_1$ and $\phi_2$ are ring homomorphisms, we get that $\phi_1(f(x)) = \phi_2(f(x))$ for any $f \in K[x]$, and therefore $\phi_1 = \phi_2$.
2. It is clear that if $f$ and $g$ are equal, their evaluations are equal for all $\alpha \in K$. Suppose now that $ev_\alpha(f) = ev_\alpha(g), \forall \alpha \in K$. By definition, this implies that the polynomial $f - g \in K[x]$ satisfies $(f-g)(\alpha) = 0, \forall \alpha \in K$. Suppose that $f - g$ is non-zero, then $f - g$ is a polynomial, say of degree $n$. On the other hand, the fact that $K[x]$ equipped with the degree function is a Euclidean domain implies that $f - g$ has root $a$ if and only if $f - g$ is divisible by $x - a$. Therefore, $f - g = \prod_{a \in K}(x - a)$. By assumption, $K$ is infinite, and therefore the degree of the right-hand side is strictly larger than $n \in \mathbb{N}$, which is a contradiction. Therefore, $f - g$

is the zero polynomial, i.e. $f = g$.
3. Consider $f(x) = x^3 + 2x$ and $g(x) = 0$. Then, $f$ and $g$ are distinct polynomials in $\mathbb{Z}_3[x]$. However, a direct computation shows that $f() = g(a) = 0, \forall a \in \mathbb{Z}_3$. $\blacksquare$