8 Divisibility of polynomials

8.1. Find irreducible decompositions in the domains $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}[x]$ of polynomials

- (a) 6x 6,
- (b) $2x^2 + 2$.

Solutions: (a) irreducible in $\mathbb{R}[x]$, $\mathbb{C}[x]$, $2 \cdot 3 \cdot (x-1)$ in $\mathbb{Z}[x]$, (b) irreducible in $\mathbb{R}[x]$, $(2x+2i) \cdot (x-i)$ in $\mathbb{C}[x]$, $2 \cdot (x^2+1)$ in $\mathbb{Z}[x]$.

8.2. Calculate gcd(f, g) in $\mathbb{Z}[x]$ if

- (a) $f = 6x^3 6, g = 8x^2 8,$
- (b) $f = 6x^2 + 3x 3, g = 6x^2 + 6x.$

Solutions: (a) 2(x-1) (b) 3(x+1).

8.3. Let \mathcal{R} be a UFD, \mathcal{Q} its quotient field, $f = \sum_{i=0}^{n} a_i x^i \in R[x]$, and $\frac{r}{s} \in Q$ be a root of f such that $r, s \in R$ are coprime. Prove that

- (a) $r \mid a_0 s^n$ and so $r \mid a_0$,
- (b) $s \mid a_n r^n$ and so $s \mid a_n$.

The previous exercise proved Proposition 6.9 from the lecture notes so we can apply it to search rational roots of polynomials:

8.4. Find all rational roots of the given polynomials in $\mathbb{Z}[x]$:

(a) $3x^5 - 2x^2 + x + 1$,

(b)
$$x^3 - 7x^2 + 11x + 3$$
,

(c)
$$2x^3 - x^2 + 3$$
.

Solutions: (a) no rational root, (b) 3, (c) -1.

8.5. Let **R** be a UFD, $f = \sum_{i=0}^{n} a_i x^i$ be a primitive polynomial in **R**[x], and suppose that there exists an irreducible element $p \in R$, such that $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$, and $p^2 \nmid a_0$. Prove that f is irreducible in **R**[x].

Hint: f = gh where $g = \sum_{i=0}^{k} g_i x^i$, $h = \sum_{i=0}^{l} h_i x^i \in R[x] \setminus \{R\}$ show (a) $p \mid g_0$ or $p \mid h_0$ (b) $p \mid g_i$ by induction for i > 0 if $p \mid g_0$.

The previous assertion is called Eisenstein's criterion (Theorem 6.10 in the lecture notes).

8.6. Using either 8.3 or 8.5 prove that the following polynomials are irreducible:

- (a) $x^3 + x^2 + x + 3$ in $\mathbb{Z}[x]$,
- (b) $4x^3 15x^2 + 60x + 180$ in $\mathbb{Z}[x]$,
- (c) $\frac{10}{17}x^8 + 5x^6 + \frac{9}{2}x^5 12x^4 + \frac{4}{3}x 6$ in $\mathbb{Q}[x]$.

Hint: (a) show that the polynomial has no rational root, (b) apply the Eisenstein's criterion for the prime 5, (c) take associate polynomial in $\mathbb{Z}[x]$ which is primitive and then apply the Eisenstein's criterion for the prime 17.