5 Rings, subrings, polynomials

5.1. Let X be a set, $|X| > 1$, denote $P(X) = \{Y : Y \subseteq X\}$, and $A \div B = (A \cup B) \setminus (A \cap B)$ and $-A = A$ for each $A, B \subseteq X$.

(a) sketch the proof that $(P(X), \div, -, \cap, \emptyset)$ is a commutative ring.

(b) What is identity of the operation $\cap$?

(c) Is $(P(X), \div, -, \cap, \emptyset)$ domain?

5.2. Let $\mathcal{Z}^2 = (\mathbb{Z}^2, +, -, \cdot, (0,0))$, where $(a,b) \pm (c,d) = (a \pm c, b \pm d)$ and $(a,b) \cdot (c,d) = (a \cdot c, b \cdot d)$. Sketch the proof that $\mathcal{Z}^2$ is a commutative ring with identity which is not a domain.

5.3. Decide for the following subsets of the filed of complex numbers $\mathcal{C} = (\mathbb{C}, +, -, \cdot, 0)$

$$\mathcal{R}_1 = \{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}, \quad \mathcal{R}_2 = \{a + b\sqrt{2} + c\sqrt{3} : \ a, b, c \in \mathbb{Z}\},$$

$$\mathcal{R}_3 = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}, \quad \mathcal{R}_4 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b, c \in \mathbb{Q}\}$$

(a) which $\mathcal{R}_i = (R_i, +, -, \cdot, 0)$, $i = 1, 2, 3, 4$, form subrings of $\mathcal{C}$,

(b) which $\mathcal{R}_i = (R_i, +, -, \cdot, 0)$, $i = 1, 2, 3, 4^\star$, form subfields of $\mathcal{C}$.

5.4. Calculate

(a) $(x^4 - 2x^3 - x^2 + x - 2) \bmod x^2 + 2$ in $\mathbb{Z}_5[x]$,

(b) $(x^4 - 2x^3 - x^2 + x - 2) \operatorname{div} x^2 + 2$ in $\mathbb{Z}_5[x]$,

(c) $(x^5 + 2x^3 - 3x - 2) \bmod x - 2$ in $\mathbb{Z}_7[x]$.

Solutions: (a) 4, *(b)* $x^2 + 3x + 2$, *(c) 5*

5.5. Find all roots of the polynomial

(a) $x^3 + 2x^2 + x \in \mathbb{Z}_3[x]$ in the field $\mathbb{Z}_3$,

(b) $x^2 + 1 \in \mathbb{Z}_3[x]$ in the field $\mathbb{Z}_3$,

(c) $x^2 + 1 \in \mathbb{Z}_5[x]$ in the field $\mathbb{Z}_5$,

(d) $x^6 - 1 \in \mathbb{Z}_7[x]$ in the field $\mathbb{Z}_7$,

(e) $x^6 - 1 \in \mathbb{C}[x]$ in the field $\mathbb{C}$.

Solutions: (a) $0, 2$, *(b)* $\emptyset$, *(c)* $2, 3$, *(d)* $\mathbb{Z}_7 \setminus \{0\}$, *(e)* $e^{\pi i n/3}$ *for* $n \in \mathbb{Z}_6$.