Exercise Sheet for Week 9

Question 1

In each of the following rings, which of them are commutative? Which of them admits a multiplicative inverse for every non-zero element?

- The integers $(\mathbb{Z}, +, \times)$
- The rational numbers $(\mathbb{Q}, +, \times)$
- The real numbers $(\mathbb{R}, +, \times)$
- The complex numbers $(\mathbb{C}, +, \times)$
- The matrix ring $(M_{n\times n}(\mathbb{R}), +, \times)$ for $n \in \mathbb{N} \setminus \{0\}$ (Hint: The answer to both questions may depend on n)
- The ring of matrices of non-zero determinant $(GL_n(\mathbb{R}), +, \times)$ for $n \in \mathbb{N} \setminus \{0\}$
- The congruent numbers $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ for $n \in \mathbb{N} \setminus \{0\}$ (Hint: whether all non-zero elements have a multiplicative inverse depends on n)
- The polynomial ring $\mathbb{R}[x]$

Upshot: To give you abundance of examples of rings (commutative and non-commutative), (fields / non-fields)

Question 2

The question will provide you with a ring and a subset of the ring. Which of the subsets is an ideal of the ring? Which of the subsets is a subring of the ring? (Subtle question: what is the difference between an ideal and a subring?)

- The integers $\mathbb{Z}$ and the subset $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ for some $n \in \mathbb{N} \setminus \{0\}$
- The rational numbers $\mathbb{Q}$ and the subset $\frac{5}{7}\mathbb{Z} = \{\frac{5}{7}k \mid k \in \mathbb{Z}\}$
- The congruence group $\mathbb{Z}/6\mathbb{Z}$ and the subset $\{1 + \mathbb{Z}, 5 + \mathbb{Z}\}$.
- The general linear group $GL_n(\mathbb{R})$ for $n \in \mathbb{N} \setminus \{0\}$ and the subset $\{M \in GL_n(\mathbb{R}) \mid \det(M) = 1\}$
- The polynomial ring $\mathbb{R}[x]$ and the subset $\mathbb{R}$
- The polynomial ring $\mathbb{R}[x]$ and the subset $\{x - a \in \mathbb{R}[x] \mid a \in \mathbb{R}\}$

Is every subring an ideal? Is every ideal a subring? Prove or give a counter example.

Upshot: Subsets of a ring may be an ideal, may be a subring, may be neither.

Question 3

Let $(R, +, \cdot)$ be a ring. Prove of find a counter example to the following statements.

- $(R, +)$ is an abelian group
- $(R, \cdot)$ is an abelian group
- Let I be an ideal of R. Then $(I, +)$ is an abelian group
- Let $R^\times$ be the group of units in R. Then $(R^\times, +)$ is a group
- Let $R^\times$ be the group of units in R. Then $(R^\times, \cdot)$ is an abelian group

Upshot: Just a sanity check

Question 4

Find the multiplicative inverse of 17 in $\mathbb{Z}/100\mathbb{Z}$.

Upshot: Bezout's lemma comes up everywhere!

Question 5

Prove or find a counter example: Every irreducible polynomial in $\mathbb{R}[x]$ is irreducible in $\mathbb{C}[x]$.

Express $x^4 + 4x^3 + 5x^2 - 2x - 8 \in \mathbb{R}[x]$ as a product of irreducible polynomials in $\mathbb{R}[x]$. Now express the same polynomial as a product of irreducible polynomials in $\mathbb{C}[x]$.

Upshot: While factorization of a polynomial over a given polynomial ring is unique up to shuffling their factors, factorization considered over a different background ring may lead to different factorization. This is because some irreducible polynomials become reducible in a larger ambient background.