Exercise Sheet 1: Algebra

1. Let $(G, *)$ be a group. Show the following statements:

(i) the identity element is unique.

(ii) the inverse of any element is unique.

(iii) $(a^{-1})^{-1} = a$ for all $a \in G$.

(iv) $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

2. Let $((G, +), \cdot)$ be a ring. Prove the following statements:

(i) Denoting the neutral element of $+$ by 0,

$$a \cdot 0 = 0 \qquad \forall a \in G.$$

(ii) For all $a, b \in G$

$$(-a) \cdot b = -(a \cdot b), \qquad a \cdot (-b) = -(a \cdot b), \qquad (-a) \cdot (-b) = a \cdot b.$$

3. Let $((G, +), \cdot)$ be a field. Prove the following statements:

(i) For all $a, b, c \in G$

$$\Big(\ a \neq 0 \quad \text{and} \quad a \cdot b = a \cdot d \ \Big) \Longrightarrow \Big(\ b = c \ \Big).$$

(ii) Let $n \in \mathbb{N}$. If $\mathbb{Z}/n\mathbb{Z}$ is a field, then n is prime.

(*Hint: think of the definition of prime and then apply the "mod n".)*

(iii) Let $n \in \mathbb{N}$. Assume we know that $\mathbb{Z}/n\mathbb{Z}$ is a unital commutative ring. If n is prime, then $\mathbb{Z}/n\mathbb{Z}$ is a field.

(*Hint: Consider all multiples of $a \in \mathbb{Z}/n\mathbb{Z}$ (so, mod n). What would happen if there were $p-1$ different multiples? You can use the Fundamental Theorem of Arithmetics: "every integer greater than 1 in $\mathbb{Z}$ is prime or can be represented uniquely as a product of prime numbers (up to the order in the multiplication)".)*

4. Let V, W be vector spaces and let $L : V \to W$ be a linear map. Show the following:

(i) $\ker L$ is a vector subspace of V.

(ii) $\operatorname{Im} L$ is a vector subspace of W.

(iii) L is injective *if and only if* $\ker L = \{0\}$.

(iv) If $\dim(V) = \dim(W) < +\infty$, then L is injective *if and only if* it is surjective.

(*Since we did not have time to see the rank nullity theorem, use an isomorphism with $\mathbb{R}^n$ and the notion of bases.)*

5. Let V, W be finite dimensional real vector spaces. Prove the following claims:

(i) $\mathbb{C}$ (as a real vector space) $\cong \mathbb{R}^2$.

(ii) There exists some $n \in \mathbb{N}$ such that $V \cong \mathbb{R}^n$.

(iii) $\{L : V \to W \mid L \text{ is linear}\} \cong \mathbb{R}^{dim(V) \times \dim(W)}$.