ProblemSet 1 – Commutative rings & polynomials

George McNinch

2025-01-24

1. Let $p, q \in \mathbb{Z}$ be integers and consider the assignment

$$\phi : \mathbb{Z} \to \mathbb{Z}/\langle p \rangle \times \mathbb{Z}/\langle q \rangle$$

given for $a \in \mathbb{Z}$ by the rule $\phi(a) = ([a],[a]) = (a + \langle p \rangle, a + \langle q \rangle)$.

   a. Show that ϕ is a ring homomorphism. [1]

   b. Assume that $\gcd(p,q) = 1$. We will later show that there are integers $u, v \in \mathbb{Z}$ for which $up + vq = 1$. Use this to show that ϕ is *surjective* in this case.

   c. Show that ϕ is not surjective when $p = q$.

2. Consider the set $R = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.

   a. Show that R is a ring by showing that R is a *subring* of $\mathbb{R}$. [2]

   Consider the polynomial $f(T) = T^2 - 5 \in \mathbb{Q}[T]$. It is a fact that

$$(\clubsuit) \quad f(\alpha) = \alpha^2 - 5 \neq 0 \quad \text{for every } \alpha \in \mathbb{Q}.$$

   (We'll have efficient arguments for this later on).

   b. Use the result ($\clubsuit$) to show for $a, b \in \mathbb{Q}$ that $a + b\sqrt{5} = 0 \implies a = b = 0$.

   c. Use the result ($\clubsuit$) to show that if $0 \neq \alpha \in R$ then $\alpha^{-1} = \dfrac{1}{\alpha} \in R$.

3. A commutative ring R is called a *field* if every non-zero element of R has a multiplicative inverse.

   A non-zero element x of a commutative ring R is called a zero-divisor if there is a non-zero element $y \in R$ for which $xy = 0$.

   a. If F is a field, show that F contains no zero divisors.

   b. A commutative ring with no zero divisors is called an *integral domain*. Show that any subring of a field is an integral domain. Conclude that $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{5}]$ are all integral domains.

   c. If R is any commutative ring (with identity), show that the cartesian product $R \times R$ is a commutative ring which is never an integral domain.

   d. Show for any integer $n > 1$ that the ring $\mathbb{Z}/\langle n^2 \rangle$ is not an integral domain.

4. Let F be a field and let $F[T]$ be the polynomial ring in the variable T with coefficients in F.

   Then $F[T]$ is a *vector space* over F (in the sense of linear algebra), and the set of monomials $\{1, T, T^2, \cdots, T^n, \cdots\}$ is a *basis* for this vector space.

   Let $\phi : F \to F$ be a ring isomorphism [3], and define a mapping $\Phi : F[T] \to F[T]$ by the rule

$$\Phi\left(\sum_{i=0}^{N} a_i T^i\right) = \sum_{i=0}^{N} \phi(a_i) T^i.$$

[1] If R and S are rings, a function $\phi : R \to S$ is a ring homomorphism if ϕ is a homomorphism of additive groups and if $\phi(ab) = \phi(a)\phi(b)$ for every $a, b \in R$.

[2] If T is a ring, a subset S of T is a subring provided that S is an additive subgroup of T and that S is closed under the multiplication obtained from T. Notice that if S is a subring, then S is itself a ring (under the operations of T).

[3] A ring homomorphism is called an isomorphism if it is invertible (as a function). The inverse function is always a ring homomorphism as well.

a. Show that Φ is a ring homomorphism.

b. Show that $\ker(\Phi) = \{0\}$ [4] and conclude that Φ is injective.

c. Show that Φ is surjective as well. Thus Φ is an isomorphism of rings (i.e. Φ is an *automorphism* of the ring $F[T]$).

   (**Hint** You can argue the surjectivity directly. Or you can argue that the image of Φ is a vector subspace of $F[T]$ containing the basis $\{T^i\}$).

---

[4] Here ker just means the kernel of Φ viewed as a homomorphism of additive groups.