26. Examples of quotient rings

In this lecture we will consider some interesting examples of quotient rings. First we will recall the definition of a quotient ring and also define homomorphisms and isomorphisms of rings.

Definition. Let R be a commutative ring and I an ideal of R. The quotient ring R/I is the set of distinct additive cosets $a + I$, with addition and multiplication defined by

$$(a + I) + (b + I) = (a + b) + I \text{ and } (a + I)(b + I) = ab + I.$$

Definition. Let R and S be rings.

(i) A mapping $\varphi : R \to S$ is called a ring homomorphism if

$$\varphi(a + b) = \varphi(a) + \varphi(b) \text{ and } \varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a, b \in R.$$

(ii) A ring isomorphism is a bijective ring homomorphism.

(iii) The rings R and S are called isomorphic if there exists a ring isomorphism $\varphi : R \to S$.

Example 1: Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ for some $n > 1$. Let us show that the quotient ring $R/I = \mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ (as a ring).

Proof. In the course of our study of quotient groups we have already seen that

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} \text{ as a set.}$$

Moreover, by Proposition 22.3, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ as a group with addition, and an explicit isomorphism is given by the map $\iota : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ where

$$\iota(x + n\mathbb{Z}) = [x]_n \qquad (***)$$

This means that the map $\iota : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ given by (***) is

(a) well-defined

(b) bijective

(c) preserves group operation (addition), that is,

$$\iota((x + n\mathbb{Z}) + (y + n\mathbb{Z})) = \iota((x + y) + n\mathbb{Z}) \text{ for all } x, y \in \mathbb{Z}$$

We claim that ι is actually a ring isomorphism. In view of (a), (b) and (c) it remains to check that ι also preserves multiplication, which can be done directly (using the definition of multiplication in both $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_n$):

$$\iota((x + n\mathbb{Z})(y + n\mathbb{Z})) = \iota(xy + n\mathbb{Z}) = [xy]_n = [x]_n[y]_n = \iota(x + n\mathbb{Z})\iota(y + n\mathbb{Z}).$$

□

Remark: We could give a proof without referring to Proposition 22.3, by checking conditions (a), (b) and (c) directly, which is not difficult.

Example 2: Let $R = \mathbb{R}[x]$, the ring of polynomials with real coefficients and $I = (x^2+1)R = \{(x^2+1)f : f \in R\}$, the principal ideal of R generated by x^2+1. Let us prove that the quotient ring $R/I = \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is isomorphic to $\mathbb{C}$ (complex numbers).

We start with a very important result about polynomials which is an analogue of division with remainder for integers:

Theorem 26.1 (Long division of polynomials)**.** *Let F be a field, and let $f, g \in F[x]$ with $g \neq 0$. Then there exist unique polynomials $q, r \in F[x]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.*

Remark: By definition, a nonzero polynomial $h \in F[x]$ has degree n if $h = a_n x^n + \ldots + a_0$ with $a_i \in F$ and $a_n \neq 0$. The degree of the zero polynomial is defined to be $-\infty$.

Proof for Example 2. We shall use the shortcut notation

$$[f] = f + I \quad \text{for} \quad f \in F[x].$$

With this notation, the formulas for addition and multiplication can be rewritten as $[f] + [g] = [f+g]$ and $[f] \cdot [g] = [fg]$. Observation 25.1 can be restated by saying that

$$[f] = [f'] \iff f' - f \in I. \qquad (***)$$

In other words, $[f] = [f'] \iff f' - f$ is divisible by x^2+1.

Lemma 26.2. *For every $f \in \mathbb{R}[x]$ there exist unique $a, b \in \mathbb{R}$ such that $[f] = [a + bx]$.*

Proof. We apply Theorem 26.1 with $g = x^2+1$. Thus, we can write $f = (x^2+1)q + r$ where $\deg(r) < \deg(x^2+1) = 2$. Hence $\deg(r) \leq 1$, so we can write $r = a + bx$ for some $a, b \in \mathbb{R}$. Since $f - r = (x^2+1)q \in I$, by (***) we have $[f] = [r] = [a + bx]$. This proves the existence part of the Lemma. The uniqueness of a and b follows from the uniqueness of the remainder in Theorem 26.1. □

Lemma 26.3. *The equality $[x]^2 = -[1]$ holds in R/I.*

Proof. This is because $[x]^2 - (-[1]) = [x^2] + [1] = [x^2+1] = [0]$ (since $x^2 + 1 \in I$). □

We are now ready to prove that R/I and $\mathbb{C}$ are isomorphic as rings. Define a map $\varphi : \mathbb{C} \to R/I$ by

$$\varphi(a + bi) = [a + bx] \text{ for all } a, b \in \mathbb{R}$$

We claim that φ is a ring isomorphism.

1. φ is well defined since every complex number is uniquely written as $a + bi$ with $a, b \in \mathbb{R}$.

2. Next we claim that φ is bijective. This follows directly from Lemma 26.2: the existence part of Lemma 26.2 implies that φ is surjective, and the uniqueness part of Lemma 26.2 implies that φ is injective (verify the details).

3. Next we check that φ preserves addition: for every $a, b, c, d \in \mathbb{R}$ we have

$$\varphi((a + bi) + (c + di)) = \varphi((a + c) + (b + d)i) = [(a + c) + (b + d)x] =$$
$$[(a + bx) + (c + dx)] = [a + bx] + [c + dx] = \varphi(a + bi) + \varphi(c + di).$$

4. Finally, we check that φ preserves multiplication. This is a bit trickier and uses Lemma 26.3. For every $a, b, c, d \in \mathbb{R}$ we have

$$\varphi((a + bi) \cdot (c + di)) = \varphi(ac - bd + (ad + bc)i) = [ac - bd + (ad + bc)x]$$

while

$$\varphi(a + bi)\varphi(c + di) = [a + bx][c + dx] = [(a + bx)(c + dx)] =$$
$$[ac + (ad + bc)x + bdx^2] = [ac + (ad + bc)x] + [bd][x^2].$$

Since $[x^2] = [x]^2 = -[1]$ by Lemma 26.3, we have

$$[ac+(ad+bc)x]+[bd][x^2] = [ac+(ad+bc)x]-[bd][1] = [(ac-bd)+(ad+bc)x].$$

Thus, $\varphi((a + bi) \cdot (c + di)) = \varphi(a + bi)\varphi(c + di)$.

Combining 1-4, we conclude that φ is a ring isomorphism. □

Another way to prove the isomorphism in Example 2 is by using FTH for rings which is formulated below.

Definition. Let $\varphi : R \to S$ be a ring homomorphism. The set $\operatorname{Ker}\varphi = \{r \in R : \varphi(r) = 0_S\}$ is called the kernel of φ.

Theorem 26.4 (FTH for rings)**.** *Let R and S be commutative rings and $\varphi : R \to S$ a ring homomorphism. Then*

(i) $\operatorname{Ker}\varphi$ *is an ideal of* R

(ii) *The quotient ring* $R/\operatorname{Ker}\varphi$ *is isomorphic to* $\varphi(R)$.

Proof. Part (i) is an easy exercise, and part (ii) is proved similarly to FTH for groups. □

Exercise: Define the map $\psi : \mathbb{R}[x] \to \mathbb{C}$ by $\psi(f) = f(i)$. Thus, ψ is the evaluation map which sends every polynomial $f \in \mathbb{R}[x]$ to its value at $x = i$. Prove that ψ is a surjective ring homomorphism and $\operatorname{Ker}\psi = (x^2+1)\mathbb{R}[x]$ and deduce that $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x] \cong \mathbb{C}$ using FTH.

Example 3: Again let $R = \mathbb{R}[x]$ and $I = (x^2-1)\mathbb{R}[x]$. Prove that the quotient ring R/I has zero divisors and therefore cannot be a field.

Proof. We will use the same general notations as in Example 2: $[f] = f + I$ for $f \in R$. Consider the elements $a = [x-1]$ and $b = [x+1]$ of R/I. Then $a \neq [0]$ since $x - 1 \notin I$ (as $x^2 - 1$ does not divide $x - 1$) and similarly $b \neq [0]$ since $x + 1 \notin I$. On the other hand, $ab = [x-1][x+1] = [(x-1)(x+1)] = [x^2 - 1] = [0]$. Therefore, a and b are both zero divisors. □

Definition. If A and B are rings, their direct sum $A \oplus B$ is defined as follows: as a set $A \oplus B = \{(a, b) : a \in A, b \in B\}$, and ring operations on $A \oplus B$ are defined componentwise:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \text{ and } (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

The following facts are easy to check:

(i) The zero element of $A \oplus B$ is the pair $(0_A, 0_B)$.
(ii) If A and B are both commutative, then $A \oplus B$ is also commutative
(iii) If A and B are both rings with unity, then $A \oplus B$ is also a ring with unity, and the unity of $A \oplus B$ is the pair $(1_A, 1_B)$.

Exercise: Prove that the quotient ring $R/I = \mathbb{R}[x]/(x^2 - 1)\mathbb{R}[x]$ from Example 3 is isomorphic to $\mathbb{R} \oplus \mathbb{R}$.