# 1 Quotient Rings

Recall that if H is a normal subgroup of G, then there exists a quotient group G/H defined by:

$$G/H = \{gH \mid g \in G\}$$

Where the operation of the quotient group is:

$$(q_1H)(q_2H) = (q_1q_2)H$$

## 1.1 Ideals

## Definition 1.1: Ideal

A subring A of a ring R is called a (two-sided) **ideal** of R if for every element  $r \in R$  and every  $a \in A$  then:

$$ra \in A$$
 and  $ar \in A$ 

That is,  $rA = \{ra \mid a \in A\} \subseteq A$  and  $Ar \subseteq A$ .

## Definition 1.2: Proper Ideal

An ideal A is called **proper** if  $A \subset R$ .

## 1.1.1 Example 1: Even Integers

 $2\mathbb{Z} \subseteq \mathbb{Z}$  is an ideal. Suppose that there is some integer  $r \in \mathbb{Z}$  and  $a \in 2\mathbb{Z}$ . Then, a = 2k for some  $k \in \mathbb{Z}$  so that  $ra = r \cdot 2k = 2(rk) \in 2\mathbb{Z}$ . Note that this also extends to any  $n\mathbb{Z}$ ; that is,  $n\mathbb{Z}$  is an ideal.

## 1.1.2 Example 2: Trivial Subring

 $\{0\} \subseteq R$  is a trivial ideal because  $r\{0\} = \{0\}r = \{0\}$ .

## 1.1.3 Example 3: Integers/Rationals

 $\mathbb{Z} \subseteq \mathbb{Q}$  is not an ideal. Take  $r = \frac{1}{2} \in \mathbb{Q}$  and  $a = 1 \in \mathbb{Z}$ . Then:

$$ra = \frac{1}{2}(1) = \frac{1}{2} \notin \mathbb{Z}$$

#### 1.2 Ideal Test

## Theorem 1.1: Ideal Test

A nonempty subset  $A \subseteq R$  is an ideal if and only if:

- $1. \ a,b \in A \implies a-b \in A.$
- $2. \ a \in A, r \in R \implies ra, ar \in R.$

*Proof.* This is similar to the subring test.

## 1.3 Principal Ideal

If R is a commutative ring with unity, then the principal ideal generated by  $a \in R$  is:

$$\langle a \rangle = (a) = \{ ra \mid r \in R \}$$

*Proof.* Pick two elements  $ra, sa \in \langle a \rangle$ . Then,  $ra - sa = (r - s)a \in \langle a \rangle$ . Likewise, if  $r \in R$ , then  $sa \in \langle a \rangle$  so:

$$(sa)r = r(sa) = (rs)a \in \langle a \rangle$$

So, we are done.

## 1.3.1 Example 4: Integers

Consider  $R = \mathbb{Z}$  with  $\langle n \rangle = n\mathbb{Z}$ . This is a principal ideal.

### 1.3.2 Example 5: Polynomials

If  $R = \mathbb{R}[x]$ , then:

$$\langle x \rangle = \{ f(x)x \mid f(x) \in \mathbb{R}[x] \}$$

$$= \{ \text{Polynomials divisible by } x \}$$

$$= \{ f(x) \in \mathbb{R}[x] \mid f(0) = 0 \}$$

## 1.3.3 Example 6: Ring of Unity

The ideal generated by  $a_1, a_2, \ldots, a_n \in R$ , where R is a commutative ring of unity, is:

$$\langle a_1, a_2, \dots, a_n \rangle = \{ r_1 a_1 + r_2 a_2 + \dots + r_n a_n \mid r_1, \dots, r_n \in R \}$$

## 1.3.4 Example 7: Two Elements

Consider  $\langle 2, x \rangle \subseteq \mathbb{Z}[x]$ . This is defined by:

$$\{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even.}\}$$

#### 1.3.5 Problem 1: Ideal

Consider  $I = \langle a_1, a_2, \dots, a_n \rangle = \{r_1 a_1 + \dots + r_n a_n \mid r_i \in R\}$ . Show that this is an ideal.

*Proof.* We use the ideal test.

- 1. If we take two elements  $a, b \in I$ , then it's trivial to see that  $a b \in I$ .
- 2. Likewise, if we took  $a \in I$  and  $r \in R$ , then it's trivial to see that  $ra \in I$ .

So, we are done.

## 1.4 Quotient Groups

## Definition 1.3: Quotient Group

Let  $I \subseteq R$  be an ideal of R. Then, the **quotient ring** (or factor ring) is the set of cosets

$$R/I = \{r + I \mid r \in R\}$$

with the operations

$$(r+I) + (s+I) = (r+s) + I$$
  
 $(r+I)(s+I) = (rs) + I$ 

**Proposition.** R/I is a ring.

*Proof.* • For addition, we know that (R, +) is an abelian group. This implies that (I, +) is a normal subgroup of (R, +), so (R/I, +) is a group.

• For multiplication, suppose r + I = r' + I and s + I = s' + I, i.e.

$$r = r' + a$$
 and  $s = s' + b$  for some  $a, b \in I$ 

Then, (rs) = (r'+a)(s'+b) = r's' + r'b + as' + ab. Note that r'b, as', ab all belong to the ideal. So  $r's' + r'b + as' + ab \in r's' + I$ .

And, we are done.

### 1.4.1 Example 1: Integers Modulo 5

Consider  $\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$ . We know that  $5\mathbb{Z} \subseteq \mathbb{Z}$  is an ideal.

## 1.4.2 Example 2: Polynomial Ideal

Consider  $\mathbb{R}[x]/\langle x^2+1\rangle$ . This ring is "isomorphic" to  $\mathbb{C}$ . By identifying  $x+\langle x^2+1\rangle\in\mathbb{R}[x]/\langle x^2+1\rangle$  as  $i\in\mathbb{C}$ , then:

$$(x + \langle x^2 + 1 \rangle)^2 = x^2 + \langle x^2 + 1 \rangle = x^2 + -(x^2 + 1) + \langle x^2 + 1 \rangle = -1 + \langle x^2 + 1 \rangle$$

We can also see this through polynomial long division. There is a unique way to write f(x) = g(x)q(x) + r(x) with deg  $r(x) < \deg g(x)$ . From this, we can tell that:

$$f(x) + \langle x^2 + 1 \rangle = (x^2 + 1)q(x) + (a + bx) + \langle x^2 + 1 \rangle = (a + bx) + \langle x^2 + 1 \rangle$$

#### 1.4.3 Example 3: Gaussian Integers

Take  $\mathbb{Z}[i]/(2-i)$ . We claim that this is "isomorphic" to  $\mathbb{Z}/5\mathbb{Z}$ . It turns out:

$$\mathbb{Z}[i]/\langle 2-i\rangle = \{0+\langle 2-i\rangle, 1+\langle 2-i\rangle, 2+\langle 2-i\rangle, 3+\langle 2-i\rangle, 4+\langle 2-i\rangle\}$$

Consider that  $2 + \langle 2 - i \rangle = i + \langle 2 - i \rangle$  because  $2 - i \in \langle 2 - i \rangle$ . Then:

$$2^{2} + \langle 2 - i \rangle = i^{2} + \langle 2 - i \rangle$$

$$\implies 4 + \langle 2 - i \rangle = -1 + \langle 2 - i \rangle$$

$$\implies 5 \in \langle 2 - i \rangle$$

Thus,  $a + bi + \langle 2 - i \rangle = a + 2b + \langle 2 - i \rangle = r + \langle 2 - i \rangle$  for  $0 \le r < 5$  such that a + 2b = 5q + r. Now, how do we know that these cosets are distinct? It suffices to show that  $1 + \langle 2 - i \rangle$  has additive order 5. So:

$$5(1+\langle 2-i\rangle) = 5+\langle 2-i\rangle = 0+\langle 2-i\rangle$$

Where the last step is due to  $5 \in \langle 2-i \rangle$ . This tells us that the additive order of  $1+\langle 2-i \rangle$  divides 5. This implies that the order is either 1 or 5. If the order is 5, we are done since this implies that there are 5 distinct cosets. Otherwise, suppose towards a contradiction that  $1+\langle 2-i \rangle \in \mathbb{Z}[i]/\langle 2-i \rangle$  has additive order 1. In this case:

$$\begin{aligned} 1(1+\langle 2-i\rangle) &= 0+\langle 2-i\rangle \\ \implies 1 \in \langle 2-i\rangle &= \{(2-i)r \mid r \in \mathbb{Z}[i]\} \\ \implies 1 &= (2-i)(a+bi) \text{ for some } a,b \in \mathbb{Z} \\ \implies 1 &= 2a+2bi-ai+b \\ \implies 1+0i &= (2a+b)+(2b-a)i \\ \implies \begin{cases} 1 &= 2a+b \\ 0 &= 2b-a \end{cases} \\ \implies a &= \frac{1}{5} \text{ and } \frac{2}{5} \end{aligned}$$

However,  $a, b \in \mathbb{Z}$  so we have a contradiction and so  $1 + \langle 2 - i \rangle$  must have additive order 5.