## 25. Ideals and quotient rings

We continue our study of rings by making analogies with groups. The next concept we introduce is that of an **ideal** of a ring. Ideals are ring-theoretic counterparts of normal subgroups. Recall that one of the main reasons why normal subgroups are important is that they can be used to construct quotient groups. Similarly, ideals are special kinds of subrings, and at the end of the lecture we will see that to each ideal of a ring, one can associate a quotient ring.

While ideals can be defined in arbitrary rings, to simplify the matters we will only consider ideals in commutative rings; in fact, in all examples we will deal with commutative rings with 1.

### 25.1. Ideals.

**Definition.** Let $R$ be a commutative ring and $I$ a subset of $R$. Then $I$ is called an ideal if

(a) $I$ is a subgroup of $(R, +)$ (i.e., a subgroup with respect to addition)

(b) $I$ absorbs products with $R$. This means that for any $x \in I$ and $r \in R$ we must have $xr \in I$.

**Remark:** Note that this definition does not explicitly say that an ideal must be a subring. This, however, is an easy consequence of the definition, as we will see shortly.

**Example 1:** Let $R = \mathbb{Z}$, fix $n \in \mathbb{Z}$, and let $I = n\mathbb{Z}$ (the set of all integer multiples of $n$). Then $I$ is an ideal of $R$.

Indeed, we already know that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$, and $n\mathbb{Z}$ clearly satisfies the product absorption condition (b) (if $x$ is a multiple of $n$ and $r$ is any integer, then $xr$ is also a multiple of $n$). In fact, Example 1 is a special case of the more general Example 2:

**Example 2:** Let $R$ be any commutative ring with 1, fix $a \in R$, and let

$$I = aR = \{ar : r \in R\},$$

that is, $I$ is the set of all multiples of $a$. Then $I$ is an ideal of $R$, called the principal ideal generated by $a$. Sometimes $aR$ is denoted by $(a)$.

Let us prove that $I = aR$ is an ideal:

(a) First we prove that $I$ is a subgroup of $(R, +)$. This, in turn, boils down to the following three conditions:

(i) $I$ contains 0
(ii) $I$ is closed under addition
(iii) $I$ is closed under additive inversion

(i) holds since $0 = a \cdot 0 \in aR = I$.

(ii) Suppose that $x, y \in I$, so that $x = ar$ and $y = as$ for some $r, s \in R$. Then $x + y = ar + as = a(r + s) \in I$, so (ii) holds

(iii) If $x \in I$, then $x = ar$ for some $r \in R$, so $-x = a(-r) \in I$ as well.

(b) Now we prove the product absorption property. Take any $x \in I$ and $r \in R$. Then $x = as$ for some $s \in R$, so $xr = (as)r = a(sr) \in I$, as desired.

Let us now establish some basic properties of ideals.

**(I1)** *Every ideal of $R$ is a subring of $R$.* Recall that subrings were defined last time using the list of 4 conditions; however, the first three conditions can be combined into one condition, which says that a subring must be a subgroup of $(R, +)$. Thus, an equivalent definition of a subring is the following:

**Definition.** A subset $S$ of a ring $R$ is a subring if

(a') $S$ is a subgroup of $(R, +)$
(b') $S$ is closed under multiplication.

Comparing (a') and (b') with conditions (a) and (b) for ideals, we see that (a') is the same as (a), while (b') is a weaker version of (b). [1] Thus, the combination (a)+(b) implies the combination (a')+(b'), so (I1) holds.

Note that the converse of (I1) is false: a subring does not have to be an ideal. For instance, $\mathbb{Z}$ is a subring of $\mathbb{Q}$, but it is not an ideal of $\mathbb{Q}$ (e.g. take $x = 1 \in \mathbb{Z}$ and $r = 1/2 \in \mathbb{Q}$; then $xr = 1/2 \notin \mathbb{Z}$, so the product absorption property is violated).

**(I2)** *If $R$ is a field, then the only ideals of $R$ are $\{0\}$ and $R$ itself.* This is one of the exercises in Homework#12.

**(I3)** *Every ideal of $\mathbb{Z}$ is equal to $n\mathbb{Z}$ for some $n$.* Indeed, every ideal of $\mathbb{Z}$ must be a subgroup of $(\mathbb{Z}, +)$, and it is not hard to show that every subgroup of $(\mathbb{Z}, +)$ is equal to $n\mathbb{Z}$ for some $n$.

So far we have not seen an example of an ideal which is NOT principal, that is, not equal to $aR$ for some $a$. Property (I3) shows that every ideal of $\mathbb{Z}$ is principal, so one cannot find such examples if $R = \mathbb{Z}$. One can show

[1] Indeed, (b') only requires that the product of two elements from $S$ must be in $S$. For $S$ to have the product absorption property (b) we must start with two elements, only one of which is required to lie in $S$ (the other one must be in $R$, but not necessarily in $S$) and conclude that the product lands in $S$.

that the same property holds if $R = F[x]$ for some field $F$: every ideal of $F[x]$ is principal.

Probably the simplest commutative ring with 1 which has a non-principal ideal is $\mathbb{Z}[x]$, the ring of polynomials with coefficients in $\mathbb{Z}$.

**Exercise:** Let $I$ be the subset of $\mathbb{Z}[x]$ consisting of all polynomials whose constant term is even, that is,

$$I = \{a_0 + a_1x + \ldots + a_nx^n : \text{ each } a_i \in \mathbb{Z} \text{ and } a_0 \text{ is even. } \}$$

Prove that $I$ is non-principal ideal of $\mathbb{Z}[x]$.

**Hint:** First show that $I$ is an ideal of $R = \mathbb{Z}[x]$. Then show that for any $f \in \mathbb{Z}[x]$, the principal ideal $fR$ cannot equal $I$. It is convenient to consider three cases:

(i) $f$ is a non-constant polynomial
(ii) $f$ is an even constant
(iii) $f$ is an odd constant.

## 25.2. **Quotient rings.**

**Definition.** Let $R$ be a commutative ring and $I$ an ideal of $R$. Define the quotient ring $R/I$ as follows. As a set, $R/I$ is defined to be the set of distinct additive cosets $a + I$, with $a \in I$, where by definition

$$a + I = \{a + i : i \in I\}.$$

The addition (+) and multiplication ($\cdot$) on $R/I$ are defined by the following formulas:

$$(a + I) + (b + I) = (a + b) + I \text{ for all } a, b \in R. \tag{QA}$$

$$(a + I) \cdot (b + I) = ab + I \text{ for all } a, b \in R. \tag{QM}$$

**Remark:** The reason we are using additive cosets and not multiplicative ones is that $R$ is a group with respect to addition, but not with respect to multiplication. Moreover, $I$ is a subgroup of $(R, +)$, so additive cosets $a + I$ are precisely the cosets with respect to $I$ in the group-theoretic sense (as introduced in Lecture 19), and we can use all previously established properties of cosets in this new ring-theoretic setting.

Next recall the statement of Theorem 19.2: if $G$ is a group and $H$ is a subgroup of $G$, then for any $g, k \in G$ we have $gH = kH \iff g^{-1}k \in H$.

If $I$ is an ideal of a ring $R$, applying this statement to the group $G = (R, +)$ and its subgroup $H = I$ (and rewriting everything in the additive notation) we obtain the following useful result.

**Observation 25.1.** *Let $I$ be an ideal of a commutative ring $R$ and $x, y \in R$. Then*

$$x + I = y + I \iff y - x \in I.$$

Using Observation 25.1, we can now justify the definition of a quotient ring:

**Theorem 25.2.** *Let $R$ be a commutative ring and $I$ an ideal of $R$. Then the operations $+$ and $\cdot$ on $R/I$ given by (QA) and (QM) are well defined, and $R/I$ with these operations becomes a commutative ring.*

*Proof.* Why is addition on $R/I$ well defined? We need to prove that if $a, a', b, b' \in R$ are such that $a+I = a'+I$ and $b+I = b'+I$, then $(a+b)+I = (a'+b')+I$. By Observation 25.1, this is equivalent to proving the following implication:

$$\text{if } a' - a \in I \text{ and } b' - b \in I, \text{ then } (a' + b') - (a + b) \in I.$$

The latter is clear since $(a'+b') - (a+b) = (a'-a) + (b'-b)$ and $I$ is closed under addition.

Why is multiplication on $R/I$ well defined? By the same logic as for addition, we need to prove the following implication:

$$\text{if } a' - a \in I \text{ and } b' - b \in I, \text{ then } a'b' - ab \in I. \qquad (***)$$

So, suppose that $a' - a \in I$ and $b' - b \in I$. Then there exist $i, j \in I$ s.t. $a' = a + i$ and $b' = b + j$, and so $a'b' = (a+i)(b+j) = ab + ib + aj + ij$. By the product absorption property, $I$ contains each of the products $ib, aj$ and $ij$ (since $i, j \in I$) and hence $I$ also contains their sum $ib+aj+ij$. Therefore, $a'b' - ab = ib + aj + ij \in I$, so we proved (***).

Once we proved that the ring operations on $R/I$ are well defined, it remains to verify that they satisfy the axioms of a commutative ring. The latter is straightforward and left as an exercise (this can be done similarly to how we deduced the ring axioms for $\mathbb{Z}_n$ from the corresponding axioms for $\mathbb{Z}$). □

**Remark:** 1. Any ideal $I$ is a subgroup of $(R, +)$, and this subgroup is normal (since addition is commutative). Therefore, we can consider the quotient group $R/I$ – to distinguish it from the quotient ring we temporarily use the notations $(R/I)_{\text{ring}}$ and $(R/I)_{\text{group}}$. As our construction shows, $(R/I)_{\text{ring}} = (R/I)_{\text{group}}$ as sets; moreover, the addition on $(R/I)_{\text{ring}}$ is precisely the group operation on $(R/I)_{\text{group}}$ (which we also denote by $+$). Thus, the quotient ring $(R/I)_{\text{ring}}$ can be defined by starting with the quotient group $(R/I)_{\text{group}}$ and defining one new operation (multiplication), given by (QM).

2. Suppose that instead of assuming that $I$ is an ideal we only assumed that $I$ is a subgroup of $(R,+)$. As we just explained, this is enough to define the quotient group $(R/I,+)$, but we will not be able to define the ring structure on $R/I$ since multiplication given by (QM) will not be well defined.

**Exercise:** Let $R = \mathbb{Q}$ and $I = \mathbb{Z}$. Find $a, b, a', b' \in R$ s.t. $a + I = a' + I$ and $b + I = b' + I$, but $ab + I \neq a'b' + I$. Deduce that the multiplication on $R/I = \mathbb{Q}/\mathbb{Z}$ given by (QM) is not well defined.