Ideals: Basic Definitions and Facts

This handout is a quick reference sheet for terminology and basic facts about ideals. Throughout this sheet, R is a ring.

Definition. An **ideal** of R is a subset $I \subseteq R$ satisfying the following properties:

1. $I \neq \varnothing$ [Alternatively: $0_R \in I$.]
2. for all $x, y \in I$, we have $x - y \in I$
   [Alternatively: for all $x, y \in I$, we have $x + y \in I$ and $-x \in I$.]
3. for all $x \in I$ and all $r \in R$, we have $rx \in I$ and $xr \in I$.

Notes/Facts (suggestion: for practice, prove some or all of the claims here):

- Conditions (1) and (2) above are equivalent to saying that $(I, +)$ is a subgroup of $(R, +)$. (And informally, I call (3) the "sticky property".)
- The full ring $I = R$ is an ideal of R, called the **improper ideal** of R.
- The set $I = \{0_R\}$ is an ideal of R, called the **trivial ideal** of R.
- If $R = F$ is a field, then the **only** ideals of F are the trivial ideal and the improper ideal.
- A **subring** of R is a subset $S \subseteq R$ such that $(S, +, \cdot)$ is itself a ring. By Theorem 17.1, a subset $S \subseteq R$ is a subring if and only if S satisfies (1) and (2) above and is closed under $\cdot$ (i.e., for all $x, y \in S$, we have $xy \in S$).
  However, the sticky property (3) above is stronger than being closed under $\cdot$, since only one of the two multiplicands has to belong to the subset.
  So all ideals of R are subrings of R, but not conversely.
- **Warning**: If $S \subseteq R$ is a subring, and if $I \subseteq S$ is an ideal of S, then I might or might *not* be an ideal of R. After all, the sticky property allows the second multiplicand r to be anything in the whole ring; so if you make the ring bigger, you might break that property. For example, $2\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$, but it is *not* an ideal of the larger ring $\mathbb{Q}$.

Definitions. Let $I \subsetneq R$ be a proper ideal (of R). We say:

1. I is a **prime ideal** of R if:
   for all $x, y \in R$ such that $xy \in I$, we have $x \in I$ or $y \in I$ (or both).
2. I is a **maximal ideal** of R if there are no ideals J of R such that $I \subsetneq J \subsetneq R$.

Notes:

- Don't forget that the above definitions both require that I is a *proper* ideal.
  That is, the full ring R is neither a prime ideal nor a maximal ideal of R.
- The condition for being a prime ideal is essentially the converse of the sticky property.
  Thus, a prime ideal of R is a proper subset $I \subsetneq R$ that is a subgroup under $+$ and such that for all $x, y \in R$, we have $xy \in I$ **if and only if** either $x \in I$ or $y \in I$ (or both).
- The condition for being a maximal ideal can be rephrased as:
  For any ideal J of R with $I \subsetneq J \subseteq R$, we have $J = R$.
- **Fact**: For a nontrivial ring R, the trivial ideal $\{0_R\}$ is prime if and only if R has no nonzero zero-divisors. [Suggestion: prove that!]
- **Fact**: If R is a commutative ring with unity, and if $I \subseteq R$ is a maximal ideal of R, then I is also a prime ideal of R. [Harder to prove; see Corollary 17.8]

As I mentioned in class, subrings of a ring are (sort of) analogous to subgroups of a group, whereas ideals are (sort of) analogous to *normal* subgroups. This analogy is especially relevant to forming **quotient rings**. Just as we need a *normal* subgroup to take a quotient group, it turns out that we need an *ideal* to form a quotient ring, as follows.

Definition/Theorem. Let R be a ring, and let $I \subseteq R$ be an ideal.
Define $\boxed{R/I = \{I + a \,|\, a \in R\}}$ (i.e., the set of (right) cosets I under $+$.)

Define operations $+$ and $\cdot$ on R/I by: for all $a, b \in R$,

$$\boxed{(I+a)+(I+b) = I+(a+b)} \qquad \text{and} \qquad \boxed{(I+a)\cdot(I+b) = I+(a\cdot b)}$$

Then R/I is a ring, called the $\boxed{\textbf{quotient ring}}$ (of R modulo I). Its additive identity is $I + 0_R$. Moreover:

- If R has unity 1_R, then R/I has unity $I + 1_R$.
- If R is commutative, then R/I is commutative.

Warning: The elements of R/I are **ADDITIVE** cosets $I + a$.
NEVER write Ia or Ib for an element of R/I; there must ALWAYS be a $+$ sign.

Theorem. Let R be a **commutative ring with unity**, and let $I \subseteq R$ be an ideal. Then:

1. I is a prime ideal of R **if and only if** R/I is an integral domain.
2. I is a maximal ideal of R **if and only if** R/I is a field.

See Video 33 or Corollary 17.6 for the proof of statement (1). See Video 34 or Theorem 17.7 for the proof of statement (2). Both proofs are mainly exercises in the (admittedly confusing) definitions of prime ideals, maximal ideals, integral domains, fields, and quotient rings, as well as manipulating cosets; but the proof of (2) has extra difficulties as well. It's good practice to learn how to prove (1).

We conclude with an unrelated set of definitions that we actually could have presented earlier. (In fact, I *did* present them earlier in class.)

Definition. Let R be a **commutative ring with unity**, and let $a \in R$.
The $\boxed{\textbf{principal ideal generated by } a}$ is $\boxed{aR = \{ar \,|\, r \in R\}}$

Theorem. Let R be a commutative ring with unity, and let $a \in R$. The principal ideal aR **is** indeed an ideal of R, and $a \in aR$. Moreover, aR is the smallest ideal of R containing a, by which we mean that for any ideal I of R with the property that $a \in I$, we have $aR \subseteq I$.

Notes/Facts

- The principal ideal aR is sometimes denoted $\langle a \rangle$ or (a).
- Since we assumed R is commutative, we have $aR = Ra$, where $Ra = \{ra \,|\, r \in R\}$.
- Earlier we noted that if R is a field, then its only ideals are $\{0_R\}$ and R itself. Well, if R is a commutative ring with unity, the converse is also true: that is, if R is a commutative ring with unity whose only ideals are $\{0_R\}$ and R, then R is a field. Can you prove that? (Hint: to find a^{-1} for $a \neq 0_R$, first prove that $1_R \in aR$.)

Definition. If R is an **integral domain** with the property that all of its ideals are principal ideals, then we say that R is a $\boxed{\textbf{principal ideal domain}}$ or $\boxed{\textbf{PID}}$ for short.