Math 412. Ideals and Quotient Rings

DEFINITION: An ideal of a ring $R$ is a non-empty subset $I$ satisfying

1. If $x_1, x_2 \in I$, then $x_1 + x_2 \in I$.
2. If $x \in I$ and $r \in R$, then $rx \in I$ and $xr \in I$;

CAUTION: The book defines an ideal as a “subring” satisfying certain properties instead of a “subset.” Ideals are not usually subrings because they do not need to contain 1. Despite the difference in the language, the book’s definition does produce the same ideals as our definition above.

DEFINITION: Let $I$ be an ideal of a ring $R$. Consider arbitrary $x, y \in R$. We say that $x$ is congruent to $y$ modulo $I$ if $x - y \in I$.

DEFINITION: The congruence class of $y$ modulo $I$ is the set $\{y + z \mid z \in I\}$ of all elements of $R$ congruent to $y$ modulo $I$. We denote the congruence class modulo $I$ by $y + I$.

The set of all congruence classes of $R$ modulo $I$ is denoted $R/I$.

CAUTION: The elements of $R/I$ are sets.

DEFINITION: Let $I$ be an ideal of a ring $R$. The Quotient Ring of $R$ by $I$ is the set $R/I$ consisting of all congruence classes modulo $I$ in $R$, together with binary operations $+$ and $\cdot$ defined by

$$(x + I) + (y + I) := (x + y) + I \quad (x + I) \cdot (y + I) := (x \cdot y) + I.$$ 

A. WARM-UP. Which of the following are ideals in the given rings?

1. The set $I$ of even integers in the ring $\mathbb{Z}$.
2. The set $I$ of odd integers in the ring $\mathbb{Z}$.
3. The set $I$ of integers that can be obtained as a $\mathbb{Z}$-linear combination of the integers 18 and 24.
4. The set $I$ of integers that are divisible by both 5 and 7.
5. The set of polynomials $f$ in $\mathbb{C}[x]$ with non-zero constant term.
6. The set of polynomials $f$ in $\mathbb{Q}[x]$ with zero constant term.
7. The set of polynomials with even coefficients in $\mathbb{Z}[x]$.
8. The set of classes $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$ in the ring $\mathbb{Z}_{12}$.

Only (2) and (5) fail to be ideals.

B. EASY PROOFS.

1. In an arbitrary ring $R$, verify that the set $\{y + z \mid z \in I\}$ really is precisely the set of all elements of $R$ which are congruent to $y$ modulo $I$.
2. Is congruence modulo $I$ an equivalence relation on $R$? Explain.
3. Prove that if $x \in y + I$, then $x + I = y + I$.

(1) Say $x$ is congruent to $y$ modulo $I$. Then $x - y \in I$, so we can write $x = y + z$ where $z = x - y \in I$. So $x \in \{y + z \mid z \in I\}$. Conversely, any element of the form $y + z$ with $z \in I$ satisfies $(y + z) - y \in I$. QED.

(2) Yes! It is reflexive, symmetric and transitive; the proof is the same as we’ve done in $\mathbb{Z}$ and in $\mathbb{F}[x]$. 

(c)Karen E. Smith 2018 UM Math Dept licensed under a Creative Commons By-NC-SA 4.0 International License.
(3) Because congruence is an equivalence relation, it partitions the set \( R \) up into non-overlapping congruence classes. So if \( x \) is in the congruence class of \( y \), we know that the intersection of the classes \( x + I \) and \( y + I \) is not empty. Thus, the must be equal: \( x + I = y + I \).

C. RELATIONSHIP TO CONGRUENCE IN \( \mathbb{Z} \) AND \( \mathbb{F}[x] \)

(1) In the ring \( \mathbb{Z} \), let \( I \) be the set of multiples of some fixed \( n \in \mathbb{Z} \). Prove that \( I \) is an ideal and show that two integers are congruent modulo \( I \) if and only if they are congruent mod \( n \).

(2) In the ring \( \mathbb{Q}[x] \), let \( I \) be the set of multiples of some fixed polynomial \( f \). Prove that \( I \) is an ideal and that two polynomials are congruent modulo \( I \) if and only if they are congruent mod \( f \).

(3) Let \( I \) be the ideal of \( \mathbb{Z} \) of multiples of 20. What is the Chapter 2 notation for \( 17 + I \)? True or False: \( 17 + I = -3 + I \)? What is another notation for the set \( \mathbb{Z}/I \)?

(4) In the case \( R = \mathbb{C}[x] \), let \( I \) be the ideal of multiples of \( x^3 + x + 1 \). True or false: \( x^3 + x + I = 1 + I \)? \( ix^5 + ix^3 + ix^2 + I = 0 + I \) ? Write these statements in the Chapter 5 notation using symbols like \([g]_f \). What is another notation for \( \mathbb{C}[x]/I \)?

D. THE QUOTIENT RING \( R/I \). Fix any ring \( R \) and any ideal \( I \subset R \). Let \( R/I \) denote the set of all congruence classes modulo \( I \) in \( R \).

(1) Explain what needs to be checked in order to verify that the addition and multiplication defined above on the set \( R/I \) are well-defined. Now check it for at least one of the operations. Note: you have done this twice before!

(2) Explain briefly why the ring axioms like associativity for each operation on \( R/I \) follow easily from those for \( R \).

(3) What are the additive and multiplicative identity elements in \( R/I \)? What is the additive inverse of \( y + I \) in \( R/I \)?

(4) Prove that the canonical map \( R \rightarrow R/I \) sending each \( r \mapsto r + I \) is a surjective homomorphism. Find the kernel.

E. Let \( R = \mathbb{Z}_{6} \). Consider the subset \( I = \{[0]_6, [2]_6, [4]_6 \} \).
(1) Prove that \( I \) is an ideal of \( \mathbb{Z}_6 \).
(2) Write out the subset \([0]_6 + I\) of \( \mathbb{Z}_6 \) in set notation. Ditto for \([1]_6 + I\). Given any \([a]_6\) in \( \mathbb{Z}_6 \), what can you say about its congruence class in relation to \([0]_6 + I\) and \([1]_6 + I\)?
(3) Remember that the elements of \( R/I \) are subsets of the ring \( R \). The ring \( \mathbb{Z}/I \) has two elements, both are subsets of \( \mathbb{Z} \). Make an addition and multiplication chart for \( \mathbb{Z}/I \). What is the standard “quotient ring” notation for these elements of \( \mathbb{Z}/I \). How might you write these if we allow “abuses” of notation? What, actually, are these two elements, written out completely as a set by listing all elements.
(4) Prove that \( \mathbb{Z}/I \) is isomorphic to \( \mathbb{Z}_2 \) by describing an explicit isomorphism. Think deeply about the meaning of the elements of both \( \mathbb{Z}_2 \) and \( \mathbb{Z}/I \). In what sense are corresponding elements under the isomorphism “the same” or different?

F. GENERATORS.
(1) Fix any elements \( c_1, c_2, \ldots, c_t \) in a commutative ring \( R \). Show that the set
\[
\{ r_1 c_1 + r_2 c_2 + \cdots + r_t c_t \mid r_i \in R \}
\]
of \( R \)-linear combinations of the \( c_i \) is an ideal of \( R \). We denote this ideal by \( (c_1, c_2, \ldots, c_t) \), and call it the ideal generated by \( c_1, c_2, \ldots, c_t \).
(2) Show that if \( c \in R \) is arbitrary and \( u \in R \) is a unit, then \( (c) \) and \( (uc) \) are the same ideal of \( R \).

G. KERNEL IS AN IDEAL. Let \( \phi : R \to S \) be a ring homomorphism. Prove that \( \ker \phi \) is an ideal of \( R \).

H. PRODUCTS. Let \( R \times S \) be a product of two rings.
(1) Show that the set \( I = R \times \{0_S\} = \{(r, 0_S) \mid r \in R\} \) is an ideal of \( R \times S \).
(2) Prove that \( (r_1, s_1) \) is congruent modulo \( I \) to \( (r_2, s_2) \) if and only if \( s_1 = s_2 \).
(3) Prove that every congruence class of $R \times S$ modulo $I$ contains exactly one element of the form $(0_R, s)$ where $s \in S$.

(4) Prove that the map $S \rightarrow (R \times S)/I$ sending $s \mapsto (0_R, s) + I$ is a ring isomorphism.

(5) Prove that the map $R \times S \rightarrow S$ sending $(r, s) \mapsto s$ is a surjective ring homomorphism with kernel $I$.

I. Ideals in fields. Let $F$ be a field. Prove that the only ideals in $F$ are $\{0\}$ and $F$. Prove that every ring homomorphism $F \rightarrow R$ is injective.