Math 412. Adventure sheet on ideals

DEFINITION: An **ideal** of a ring R is a nonempty 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: When reading the text, you will see an ideal defined as a certain kind of "subring". DO NOT USE THIS DEFINITION! Remember that for us, a subring always contains 1, because all rings contain 1. But most ideals do not contain 1.

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 $y + I$.

A. A WARM-UP TO THE WARM-UP. Check the following are true:

(1) Every ideal contains 0.
(2) Ideals are closed under additive inverses.
(3) If $1 \in I$, then $I = R$.

B. 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 of polynomials f in $\mathbb{C}[x]$ with nonzero constant term.
(5) The set of polynomials with even coefficients in $\mathbb{Z}[x]$.
(6) The set of classes $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$ in the ring $\mathbb{Z}_{12}$.

C. EASY PROOFS. Fix a commutative ring R and an ideal I.

(1) Prove that the kernel of a ring homomorphism $R \xrightarrow{\phi} S$ is an ideal of R.
(2) 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.
(3) Verify that congruence modulo I is an equivalence relation on R.

D. PRINCIPAL IDEALS. Fix a commutative ring R and fix some $c \in R$. Let I be the set $(c) := \{rc \mid r \in R\}$ of all multiples of c.

(1) Prove that I is an ideal. We call this the **principal ideal** generated by c.
(2) Let R be a commutative ring, and $r, s \in R$. When is $(r) \subseteq (s)$? When is $(r) = (s)$?
(3) Show that a is congruent to b modulo I if and only if c divides $a - b$ in R.[1]
(4) In the case $R = \mathbb{Z}$, fix $c = 20$. In common language from high school, what is the principal ideal generated by 20? What is another notation for $17 + I$?
(5) Let $R = \mathbb{Z}[x]$, and I be the set of polynomials in R such that $f(0)$ is an even integer. Show that I is an ideal, but that I is *not* a principal ideal for any choice of c.[2]

[1] $x|y$ in R if there exists a $z \in R$ such that $xz = y$.
[2] Hint: $2 \in I$ and $x \in I$.

E. IDEALS IN $\mathbb{Z}$ AND $\mathbb{F}[x]$.

(1) Let I be an ideal in $\mathbb{Z}$, and suppose that $I \neq \{0\}$. Prove that $I = (c)$, where c is the smallest positive integer in I. Conclude that every ideal in $\mathbb{Z}$ is a principal ideal.
(2) Let $\mathbb{F}$ be a field, and $R = \mathbb{F}[x]$. Let I be an ideal in R, and suppose that $I \neq \{0\}$. Prove that $I = (f(x))$, where $f(x)$ is the monic polynomial of smallest degree in I. Conclude that every ideal in R is a principal ideal.
(3) Is every ideal in every ring a principal ideal?

F. GENERATORS.

(1) Fix any elements $c_1, c_2, \dots, c_t$ in a commutative ring R. Show that the set
$$\{r_1c_1 + r_2c_2 + \cdots + r_tc_t \mid r_i \in R\}$$
of R-linear combinations of the c_i is an ideal of R. We denote this ideal by $(c_1, c_2, \dots, c_t)$, and call it the **ideal generated by** $c_1, c_2, \dots, c_t$.
(2) Let $m, n \in \mathbb{Z}$. We know that the ideal generated by m and n is principal. What is a (single) generator for this ideal?
(3) Let $f, g \in \mathbb{F}[x]$. We know that the ideal generated by f and g is principal. What is a (single) generator for this ideal?
(4) Find generators for the ideal considered in D5.
(5) Consider the ideal $(x, y) \subseteq \mathbb{R}[x, y]$. Is it principal?

G. 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 $R \times S \to S$ sending $(r, s) \mapsto s$ is a surjective ring homomorphism with kernel I.

H. IDEALS IN FIELDS.

(1) Let I be an ideal in a ring R. Prove that if $1_R \in I$, then $I = R$.
(2) Prove that if $\mathbb{F}$ is a field, then its only ideals are $\{0\}$ and $\mathbb{F}$.
(3) Prove that if $\mathbb{F}$ is a field and R is a ring in which $0 \neq 1$, then every ring homomorphism $\mathbb{F} \xrightarrow{\phi} R$ is injective.