Math 412. 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". $\ast\star$**Do not use this definition!**$\ast\star$ 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 $x - y \in I$. In this case, we write $x \equiv y \pmod{I}$.

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 $y + I$.

Part 1: Getting acquainted.

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 $\mathbb{Z}_{12}$.

Solution. (2) and (4) are not ideals, but all the other ones are.

C. INTRODUCTORY 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.

Solution.

(1) The kernel is nonempty because it always contains 0. If $\phi(x) = \phi(y) = 0$, then $\phi(x + y) = \phi(x) + \phi(y) = 0$. Also, given any $r \in R$, $\phi(rx) = \phi(r)\phi(x) = 0$.
(2) $x \in R$ is congruent to y modulo I if and only if $x - y \in I$, or equivalently if $x - y = z$ for some $z \in I$, that is $x = y + z$ for some $z \in I$.
(3) The proof is the same as what we have done over $\mathbb{Z}$ and $\mathbb{F}[x]$.

Part 2: Looking forward.

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]

Solution.

(1) Given $r, s \in R$, $rc + sc = (r + s)c \in I$. Given any $r, s \in I$, $s(rc) = (sr)c \in I$. Also I is nonempty because $c \in I$.
(2) $(r) \subseteq (s)$ if and only if $s|r$. $(r) = (s)$ if and only if $r|s$ and $s|r$. If R also happens to be a domain, this means that $r = us$ for some unit u.
(3) By definition, a is congruent to b if $a - b \in I$, which is equivalent to saying $a - b = rc$, which is equivalent to saying c divides $a - b$.
(4) The principal ideal generated by 20 is the set of multiples of 20. Another notation for $17 + I$ is $[17]_{20}$.
(5) We prove this by contradiction. If $I = (c)$ for some c, then $c|2$ and $c|x$. Since $c|2$, we know that c is a constant. Then, c is a constant that divides 2, so $c = \pm 1, \pm 2$. But, x is not a multiple of ± 2 in $\mathbb{Z}[x]$, so $I = (1)$. But this is a contradiction, since $1 \notin I$!

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?

Solution.

(1) Note first that I contains a positive integer, since it contains some nonzero integer, and it is closed under "negatives." We need to show that if $x \in I$, then $c|x$. Use the division algorithm to write $x = cq + r$, with $0 \leq r < c$. Since $c \in I$, $cq \in I$. Since $cq \in I$, $-cq \in I$. Since $-cq \in I$ and $x \in I$, $r = x - cq \in I$. By definition of c, we must have $r = 0$, so $c|x$.
(2) The proof is analogous to the previous part, just using the division algorithm for polynomials instead!
(3) No!

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

Part 3: Going Deeper/Combining ideas.

F. GENERATORS.

(1) Fix any elements $c_1, c_2, \ldots, c_t$ 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 $(c_1, c_2, \ldots, c_t)$, and call it the **ideal generated by** $c_1, c_2, \ldots, c_t$.

(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?

Solution.

(1) We need to show that this is closed under addition, and absorbs multiplication. Let $x, y \in (c_1, c_2, \ldots, c_t)$. Write $x = r_1c_1 + r_2c_2 + \cdots + r_tc_t$ and $y = s_1c_1 + s_2c_2 + \cdots + s_tc_t$. Then

$$x+y = r_1c_1+r_2c_2+\cdots+r_tc_t+s_1c_1+s_2c_2+\cdots+s_tc_t = (r_1+s_1)c_1+(r_2+s_2)c_2+\cdots+(r_t+s_t)c_t,$$

which is in $(c_1, c_2, \ldots, c_t)$. Similarly, for $a \in R$, we have

$$ax = a(r_1c_1+r_2c_2+\cdots+r_tc_t) = ar_1c_1+ar_2c_2+\cdots+ar_tc_t = (ar_1)c_1+(ar_2)c_2+\cdots+(ar_t)c_t,$$

which is in $(c_1, c_2, \ldots, c_t)$.

(2) The GCD of m and n! Let $d = \gcd(m, n)$. By a theorem, we know that there are elements $a, b \in \mathbb{Z}$ such that $d = am + bn$. Then, for any $c \in \mathbb{Z}$, $cd = (ca)m + (cb)n \in (m, n)$, so $(d) \subseteq (m, n)$. On the other hand, we can write $m = du$, $n = dv$ for some integers u, v, so any number of the form $am + bn$ can we written as $(au + bv)d \in (d)$, so $(m, n) \subseteq d$.

(3) The proof is analogous to the previous one!

(4) $(2, x)$

(5) No!

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.

Solution.

(1) Given $(r_1, 0)$ and $(r_2, 0)$ in I, we have $(r_1, 0) + (r_2, 0) = (r_1 + r_2, 0) \in I$, and given $(r_1, 0) \in I$ and $(a, b) \in R \times S$, we have $(a, b)(r_1, 0) = (ar_1, 0) \in I$.

(2) (r_1, s_1) is congruent to (r_2, s_2) modulo I if and only if $(r_1, s_1) - (r_2, s_2) = (r_1 - r_2, s_1 - s_2) \in I$; equivalently $s_1 - s_2 = 0$, or $s_1 = s_2$, by the definition of I.

(3) We must show that any $(a, b) \in R \times S$ is congruent modulo I to exactly one element of the form $(0, s)$ for $s \in S$; indeed, by the previous part, this is true exactly for $s = b$.

(4) The map is clearly surjective, and is easily checked to be a ring homomorphism. An element (r, s) is in the kernel if and only if $s = 0$, i.e. if and only if $(r, s) \in I$.

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.

Solution.

(1) For any $r \in R$, we have $r = 1 \times R$, so $r \in I$ by the absorption property.

(2) If $I \neq \{0\}$, there is some $s \neq 0$ in I. Then, for any $r \in \mathbb{F}$, we can write $r = (rs^{-1})s$, so $r \in I$ by the absorption property.

(3) The kernel is an ideal, and is not all of $\mathbb{F}$, since 1 is not in the kernel (1 maps to $1 \neq 0$). Thus, the kernel is zero, so the homomorphism is injective!