Math 412. Adventure sheet on quotient rings

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, which we 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 of all congruence classes modulo I in R, together with binary operations $+$ and $\cdot$ defined by

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

A. IDEALS IN SOME FAMILIAR RINGS. It turns out that we can classify ALL ideals in some special rings!

(1) Let $\mathbb{F}$ be a field. Show that the only two ideals in $\mathbb{F}$ are and $\{0\}$.
(2) 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.
(3) 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.
(4) Is every ideal in every ring a principal ideal?

Solution.

(1) Let $I \neq \{0\}$ be an ideal in $\mathbb{F}$. There exists some nonzero $c \in I$, and since $\mathbb{F}$ is a field, c is invertible. Then $1 = c^{-1}c \in I$, and that implies $I = \mathbb{F}$.
(2) Since $I \neq \{0\}$, there exists $n > 0$ in I. Consider all the elements n in I that are strictly positive, meaning $n > 0$. Every non-empty set of positive integers has a minimum element, so let n the minimum positive element in I. Given any other nonzero element $m \in I$, either m or $-m$ is positive, so we can assume without loss of generality that $m > 0$. Notice that $(n, m) = un + vm \in I$ for some $u, v \in \mathbb{Z}$. If $n \nmid m$, then $0 < (n, m) < n$, but this contradicts our assumption on n. We conclude that $n|m$ and $m \in (n)$, so $I = (n)$.

B. THE QUOTIENT RING R/I. Fix any ring R and any ideal $I \subseteq R$.

(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.
(2) Explain briefly why the ring axioms (for example, 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?
(4) What is the additive inverse of $y + I$ in R/I?
(5) Explain why R/I is commutative whenever R is commutative.

(6) Prove that the **canonical map** $R \to R/I$ sending $r \mapsto r + I$ is a *surjective homomorphism.* Find its kernel.
(7) Consider the ring $R = \mathbb{Z}$ and the ideal $I = (n)$. What is the quotient ring R/I?

Solution.

(1) Check that given any $f, g, f', g' \in R$, if $f \equiv f'$ and $g \equiv g'$, then $f + g \equiv f' + g'$ and $fg \equiv f'g'$.
(2) Whatever the statement, we can use the definitions of the operations in R/I to convert the statement we need to prove into a statement in R: for example, to prove associativity of the addition, we note that

$$((f + I) + (g + I)) + (h + I) = ((f + g) + h) + I,$$

use that the sum is associate in R, and then finally use the definition of addition in R/I again to rewrite this as $(f + I) + ((g + I) + (h + I))$.
(3) $0 + I$ and $1 + I$.
(4) $-y + I$.
(5) The multiplication operation in R/I is induced by the multiplication in R. Given any $f + I, g + I \in R/I$,

$$(f + I) \cdot (g + I) = fg + I = gf + I = (g + I) \cdot (f + I).$$

(6) It's clear this is a surjective map, so all we need to check is that it is indeed a homomorphism. Clearly, $1 \mapsto 1 + I$. The remaining properties follow by definition of the operations on R:

$$(f + I) + (g + I) = ((f + g) + I) \text{ and } (f + I) \cdot (g + I) = ((f \cdot g) + I)\,.$$

The kernel of the canonical homomorphism is I.
(7) Our old friend $\mathbb{Z}_n$.

C. 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) List out all elements of $\mathbb{Z}_6$ in the congruence classes of $[0]_6$, $[2]_6$, and $[1]_6$.
(3) Write out the subset $[0]_6 + I$ of $\mathbb{Z}_6$ in set notation. Ditto for $[1]_6 + I$.
(4) Remember that the elements of R/I are *subsets* of the ring R. The ring $\mathbb{Z}_6/I$ has **two** elements, both are subsets of $\mathbb{Z}_6$. What are these two elements in this case? What is the standard "quotient ring" notation for these elements of $\mathbb{Z}_6/I$? What is the simplest possible notation for these two elements of $\mathbb{Z}_6/I$, allowing "abuses" of notation?
(5) Prove that $\mathbb{Z}_6/I \cong \mathbb{Z}_2$ by describing an explicit isomorphism. Think about how the corresponding elements of $\mathbb{Z}_2$ and $\mathbb{Z}_6/I$ under the isomorphism are "the same" or different.

Solution.

(1) This is a non-empty subset of $\mathbb{Z}_6$. It's closed for additive inverses because $-[2]_6 = [4]_6$, closed for addition because $[2] + [2] = [4]$, $[2] + [4] = [0]$ and $[4] + [4] = [2]$, and closed for multiplication by any elements because as a subset of $\mathbb{Z}$, the union of all these classes corresponds precisely to all the even integers.
(2) $[0]_6 + I = [2]_6 + I = \{[0]_6, [2]_6, [4]_6\}$ and $[1]_6 + I = [2]_6 + I = \{[1]_6, [3]_6, [5]_6\}$. There are only two elements in $\mathbb{Z}_6/I$.
(3) Same answer as the previous question.

(4) The two elements we already described. We could simplify our notation and writing them as just $0 + I$ and $1 + I$, or even just 0 and 1.
(5) Check that the map $[0]_6 + I \mapsto [0]_2$ and $[1]_6 + I \mapsto [1]_2$ is a ring homomorphism. This is also easily a bijection.

D. QUOTIENTS OF POLYNOMIAL RINGS.

(1) Let $\mathbb{F}$ be a field, and $R = \mathbb{F}[x]$. Let $I = (f(x)) = \{g(x)f(x) \mid g(x) \in R\}$ be an ideal. Show that every element $h(x) + I \in R/I$ contains exactly one polynomial $t(x)$ such that $t(x) = 0$ or $\deg(t(x)) < \deg(f(x))$.
(2) How many elements are in $\mathbb{Z}_2[x]/(x^2 + x + 1)$?
(3) Write out addition and multiplication tables for the quotient ring in the previous part. Is it a domain? Is it a field?
(4) Prove, in general, that if $\mathbb{F}$ is a field, $R = \mathbb{F}[x]$, and $f(x)$ is irreducible, then $R/(f(x))$ is a field.

Solution.

(1) Notice that there is only one such polynomial in I: 0. Given two such polynomials $t(x), u(x), t(x) - u(x)$ is also such a polynomial. Therefore, if $t(x) \equiv u(x)$ modulo I, that means that $t(x) - u(x) = 0$. This shows that each polynomial $t(x)$ such that $t(x) = 0$ or $\deg(t(x)) < \deg(f(x))$ determines a different class modulo I. Now it remains to check that these are all the equivalence classes. But given any polynomial $h(x)$, if $r(x)$ is the remainder when we divide $h(x)$ by $f(x)$, then $h(x) \equiv r(x)$ and $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$.
(2) There is a class for each polynomial of degree strictly less than 2, and there are 4 such polynomials: $0, 1, x, x + 1$.
(3) Not a domain nor a field.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	x

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	x
$x+1$	0	$x+1$	x	1

(4) Following what we did for $\mathbb{Z}$, we can show that the greatest common divisor between two elements f and g in $\mathbb{F}[x]$ can be obtained from a factorization into irreducibles: if

$$f = uf_1 \cdots f_n \text{ and } g = vg_1 \cdots g_m$$

for monic irreducible polynomials f_j, g_i and units u, v, then the greatest common divisor of f and g is simply the product of all the common irreducible factors, counting minimum common multiplicity. Consider any $g \in \mathbb{F}[x]$, and suppose that $g = ug_1 \cdots g_n$ is a factorization into monic irreducibles with u a unit. If $g + (f) \neq 0 + (f)$, then $f \nmid g$, and thus $f \nmid g_i$ for all i. Then the greatest common divisor of f and g is 1, and $pf + qg = 1$ for some polynomials p and q. Then $q + I$ is the multiplicative inverse of $g + I$ in R/I.

E. IDEALS IN QUOTIENT RINGS. The ideals in R/I are in one-to-one correspondence with the ideals in R that contain I.

(1) Suppose that $J \supseteq I$ is an ideal in R. Show the image of J by the canonical homomorphism $\pi : R \longrightarrow R/I$ is an ideal in R/I.
(2) Consider any ideal a in R/I. Show that the set

$$J = \pi^{-1}(a) = \{r \in R : r + I \in a\}$$

is an ideal in R that contains I.
(3) What are the ideals in $\mathbb{Z}_{42}$? What ideals in $\mathbb{Z}$ do they correspond to?

Solution.

(1) Since $0 \in J$, $0 + I \in \pi(J)$. Given any $r, s \in J$, and any $t \in R$,

$$\pi(r) + \pi(s) = \pi(r + s) \in \pi(J), -\pi(r) = \pi(-r) \in \pi(J),$$

and

$$(t + R)\pi(a) = \pi(t)\pi(a) = \pi(ta) \in \pi(J).$$

Notice that we used here the fact that π is surjective.
(2) Clearly, $0 \in J$. If $r, s \in J$ and $t \in R$, then

$$(r+s)+I = (r+I)+(s+I) \in a, -r+I = -(r+I) \in a, \text{ and } ts+I = (t+I)(s+I) \in a,$$

since a is an ideal, and thus $r + s, ts \in J$. Therefore, J is an ideal. Moreover, if $r \in I$, then $r + I = 0 + I \in a$, so $I \subseteq J$.
(3) Since $42 = 2 * 3 * 7$ and $(n) \supseteq (42)$ if and only if $n|42$, there are three nontrivial ideals in $\mathbb{Z}_{42}$: $([2]_{42})$, $([3]_{42})$, and $([7]_{42})$.