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?

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?

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.

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.

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?