Math 412. 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 $x - y \in I$. 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, 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

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

Part 1: Getting acquainted.

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 $\mathbb{F}$ 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) 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 $c|x$.
(3) The proof is analogous to the previous part, just using the division algorithm for polynomials instead!
(4) No — see problem D(5) of worksheet 10 for an example.

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.

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.

Part 2: Understanding examples.

C. REVIEW: QUOTIENTS OF $\mathbb{Z}$.

(1) Consider the ring $R = \mathbb{Z}$ and the ideal $I = (n)$. What is the quotient ring R/I?
(2) Let $I = (8)$. Cacluate $(2 + I) \cdot (5 + I)$ in $\mathbb{Z}/I$.
(3) Let $n \in \mathbb{Z}$ with $n > 1$. For which n is the quotient ring $\mathbb{Z}/(n)$ a field?

Solution.

(1) Our old friend $\mathbb{Z}_n$.
(2) $(2 + I) \cdot (5 + I) = 10 + I = 2 + I$
(3) $\mathbb{Z}/(n) = \mathbb{Z}_n$ is a field if and only if n is prime.

D. 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 $[1]_6$ modulo I.
(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 $[1]_6 + I = \{[1]_6, [3]_6, [5]_6\}$. 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.

E. Quotients of polynomial rings.

(1) Let $R = \mathbb{Z}_2[x]$. Let $I = (x^2) = \{g(x)x^2 \mid g(x) \in R\}$ be an ideal. Find an element of $x^5 + x^3 + x^2 + x + I$ of degree 1.

(2) Find an element in $(x+I)\cdot(x+1+I)$ of degree 1.

(3) Show that every element $h(x) + I \in R/I$ contains exactly one polynomial $t(x)$ such that $t(x) = 0$ or $\deg(t(x)) < 2$.

(4) How many elements are in $\mathbb{Z}_2[x]/(x^2)$?

(5) Write out addition and multiplication tables for the quotient ring $\mathbb{Z}_2[x]/(x^2)$. Is it a domain? Is it a field? What is its characteristic?

(6) Does your proof for c work if $I = (x^2+x+1)$? How many elements are in $\mathbb{Z}_2[x]/(x^2 + x + 1)$?

(7) Write out addition and multiplication tables for the quotient ring $\mathbb{Z}_2[x]/(x^2+x+1)$. Is it a domain? Is it a field? What is its characteristic?

(8) Let $I = (g(x))$. Show that $\gcd(f(x), g(x)) = 1$ if and only if $f(x) + I$ is a unit in $\mathbb{F}[x]/I$ (remember the analog of Bézout's identity for polynomial rings).

(9) Make a conjecture: if $\mathbb{F}$ is a field, $R = \mathbb{F}[x]$ then $R/(f(x))$ is a field if $f(x)$ is ...

Solution.

(1) $x^5 + x^3 + x^2 + x + I = x + I$, because $x^5 + x^3 + x^2 \in I$.

(2) First we see that $(x+I)\cdot(x+1+I) = x^2+x+I$. Since $x^2 \in I$, $x^2+x+I = x+I$.

(3) We've done this before on the polynomial ring worksheet! By the division algorithm on polynomials, we can write

$$h(x) = q(x)x^2 + t(x)$$

where $t(x)$ is 0 or a polynomial of degree strictly less than 2. Thus $h(x) - t(x) = q(x)x^2$, so $h(x) + I = t(x) + I$.

Furthermore, to show uniqueness, suppose that $t_1(x), t_2(x)$ are both polynomials such that $t_i(x) = 0$ or $\deg(t_i(x)) < 2$, and suppose that $t_1(x) \in h(x) + I$ and $t_2(x) \in h(x) + I$. Then $t_1(x) + I = t_2(x) + I$, so $t_1(x) - t_2(x) \in I$. Thus $t_1(x) - t_2(x) = g(x)\cdot x^2$. If $g(x)x^2$ is not zero, then $g(x)x^2$ has degree at least

2. But since both $t_1(x)$ and $t_2(x)$ are degree less than 2, their difference is as well. Thus it must be that $g(x)x^2 = 0 = t_1(x) - t_2(x)$.

(4) There are 4 elements in $\mathbb{Z}_2/(x^2)$.

(5)

$+$	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	0

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

It is not a domain, nor is it a field. Its characteristic is 2.

(6) Yes, the proof works exactly the same! There are still four elements.

(7) There is a class for each polynomial of degree strictly less than 2, and there are 4 such polynomials: $0, 1, x, x+1$.

(8) A field, since $x^2 + x + 1$ is irreducible, and of characteristic 2.

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

(9) Suppose that $\gcd(f(x), g(x)) = 1$. Then there exists $u(x), v(x) \in \mathbb{F}[x]$ such that

$$u(x)f(x) + v(x)g(x) = 1.$$

Thus $u(x)f(x) - 1 = v(x)g(x)$, so $u(x)f(x) - 1 \in I$. Thus $(u(x))f(x) + I = 1 + I$, so

$$(u(x) + I)(f(x) + I) = 1 + I.$$

Now suppose that $f(x) + I$ is a unit in $\mathbb{F}[x]/I$. Then there is a $h(x) + I$ such that

$$\begin{aligned} 1 + I &= (f(x) + I)(h(x) + I) \\ &= f(x)h(x) + I. \end{aligned}$$

Thus $1 - f(x)h(x) \in I$, so there exists some $p(x)$ such that $1 - f(x)h(x) = p(x)g(x)$, which implies that

$$1 = f(x)h(x) + p(x)g(x).$$

The $\gcd(f(x), g(x))$ divides $f(x)$ and $g(x)$, so it must divide any combination of the two. Thus $\gcd(f(x), g(x))$ must be some constant, and since we define the greatest common divisor to be MONIC, we can conclude that $\gcd(f(x), g(x)) = 1$.

(10) $R/(f(x))$ is a field if $f(x)$ is irreducible.

F. More Examples

(1) True or False: If R is a domain and I is an ideal in R, then R/I is a domain.

(2) Let R and S be rings. Recall from worksheet 10G, the set $\{(r, 0_S) | r \in R\}$ is an ideal of $R \times S$. Describe the quotient ring, $(R \times S)/I$.

(3) Generate an example of a ring T and an ideal I such that T/I is a domain, but T is not a domain.

(4) True or False: If r is a unit in R and $I \neq R$, then $r + I$ is a unit in R.

Solution.

(1) False! Consider $R = \mathbb{Z}$ and $I = (4)$, or any ideal generated by an integer that is not prime.
(2) $(R \times S)/I \cong S$
(3) $\mathbb{Z}_4 \times \mathbb{Z}$ is one example. If R is not a domain and S is a domain and I is the ideal described in part (2), then $(R \times S)/I \cong S$ is a domain.
(4) True! Suppose r is a unit in R. Then there exists some $u \in R$ such that $ru = 1_R$. Thus $(r + I)(u + I) = (1 + I)$, which is the multiplicative identity in R/I.