Math 412. More 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

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

A. WARM UP

(1) Let $I = (4)$ and $R = \mathbb{Z}$. Write $(10 + I) \cdot (3 + I))$ as $a + I$ where a is the smallest positive such integer.

Solution.

$$(30 + I) = 2 + I \quad \text{ in } R/I$$

(2) Let $I = \Big((x+1)^3\Big)$ and $R = \mathbb{Z}_3[x]$. Find a polynomial in $x^3+2x^2+x+1+I$ of degree 2 or less (or the zero polynomial). You will show in part (B1) that such a polynomial is guaranteed to exist because of the division algorithm.

Solution. You showed in the homework that $\binom{3}{k}$ is divisible by 3 for $1 \le k \le 2$, so $(x+1)^3 = x^3 + 1$. Thus

$$x^3 + 2x^2 + x + 1 + I = 2x^2 + 2 + I.$$

(3) Let $R = \mathbb{R}[x]$ and let $I = (x^2 + 1)$. Find the polynomial in the product

$$(2x + 1 + I) \cdot (3x + 5 + I)$$

of degree 2 or less (or the zero polynomial).

Solution.

$$\begin{aligned}(2x+1+I)\cdot(3x+5+I) &= 6x^2 + 10x + 3x + 5 + I \\ &= 6x^2 + 6 - 1 + 13x + I \\ &= 6(x^2+1) + 13x - 1 + I\end{aligned}$$

B. 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 $\mathbb{Z}_p[x]/(f(x))$, where $f(x)$ is a polynomial of degree d?
(3) Prove that $h(x) + I$ is a zerodivisor (or zero) in $R/(f(x)) \iff \gcd(h(x), f(x)) \neq 1$.
(4) Prove that $h(x) + I$ is a unit in $R/(f(x))$ if and only if $\gcd(f(x), h(x)) = 1$. (Recall Bézout's identity for polynomials!).
(5) Prove, in general, that if $\mathbb{F}$ is a field, $R = \mathbb{F}[x]$ then $f(x)$ is irreducible if and only if $R/(f(x))$ 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 d:
$$a_0 + a_1 x + \cdots + a_n x^{d-1}$$
such that $a_i \in \mathbb{Z}_p$. Thus there are p^d many such polynomials.
(3) Suppose that $\gcd(f(x), h(x)) \neq 1$; call it $d(x)$. Then $f(x) = a(x)d(x)$ for some polynomials $a(x) \in \mathbb{F}[x]$ and $h(x) = b(x)d(x)$. Thus
$$(h(x) + I)(a(x) + I) = a(x)b(x)d(x) + I = b(x)f(x) + I = 0 + I.$$
If $a(x) + I = 0 + I$, recall that $f(x) = a(x)d(x)$, so this would imply that $d(x)$ is degree 0. But if $d(x)$ is degree 0, then it must be 1 (since gcd's are monic). Thus $a(x) + I$ is nonzero. Thus $h(x) + I$ is either $0 + I$ or a zerodivisor.

To prove the other direction, it is probably easiest to proceed by contrapositive. That is, if $\gcd(h(x), f(x)) = 1$, then $h(x) + I$ is neither a zerodivisor nor zero in $R/(f(x))$. In order to prove that $h(x) + I$ is neither a zerodivisor nor zero in $R/(f(x))$, we could show that if $(h(x) + I)(g(x) + I) = 0 + I$, then $g(x) + I$ must be 0.
So suppose that $\gcd(f(x), h(x)) = 1$. Then there exists some polynomials, $u(x)$ and $v(x)$ such that
$$u(x)f(x) + v(x)h(x) = 1.$$
Thus $v(x)h(x) + I = 1 + I$. Now suppose that
$$(h(x) + I)(g(x) + I) = 0 + I.$$
Then multiplying both sides by $(v(x) + I)$ gives
$$\begin{aligned} 0 + I &= (v(x) + I)(h(x) + I)(g(x) + I) \\ &= (v(x)h(x) + I)(g(x) + I) \\ &= (1 + I)(g(x) + I) \\ &= g(x) + I \end{aligned}$$

(4) Suppose that $\gcd(f(x), h(x)) = 1$. Then there exists some polynomials, $u(x)$ and $v(x)$ such that
$$u(x)f(x) + v(x)h(x) = 1.$$
This gives that
$$v(x)h(x) + I = 1 + I$$
so $h(x)$ is a unit!
For the other direction, if $h(x) + I$ is a unit, then there exists some $v(x) + I$ such that $h(x)v(x) + I = 1 + I$, so $h(x)v(x) - 1$ is divisible by $f(x)$. Thus there exists some $p(x)$ such that $h(x)v(x) - 1 = p(x)f(x)$, which implies that
$$h(x)v(x) - p(x)f(x) = 1.$$
Since the $\gcd(h(x), f(x))$ must divide the left side of the above equation, $\gcd(h(x), f(x)) = 1$.

(5) This follows from (3) and (4) !

C. COMPLEX NUMBERS Let $I = (x^2 + 1)$ and let $R = \mathbb{R}[x]$.

(1) Explain why every congruence class in $\mathbb{R}[x]$ modulo $x^2 + 1$ can be written in the form $a + bx + I$ for some $a, b \in \mathbb{R}$.
(2) Prove that the set of congruence classes in $\mathbb{R}[x]$ modulo $x^2 + 1$ a field.
(3) Prove that the set of congruence classes in $\mathbb{R}[x]$ modulo x^2 is *not* a field.
(4) Prove that the map $\varphi : R/I \to \mathbb{C}$ given by $\varphi(a + bx + I) = a + bi$ is well-defined.
(5) Prove that the map φ defined above is a ring homomorphism.
(6) Find the kernel of the map φ defined above. Is φ a ring isomorphism?

Solution.

(1) This follows from B1.
(2) This follows from B5. However, below is how one could prove it directly, if they so chose.
It inherits commutativity from $\mathbb{R}$, so we need only check that every nonzero element has a multiplicative inverse. Let $a+bx+I$ be some nonzero element of $\mathbb{R}[x]$ modulo $x^2 + 1$. Then $a^2 + b^2 \neq 0$ (as that only happens when $a = b = 0$). Consider
$$\begin{aligned}(a + bx)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\right) &= \frac{a^2}{a^2 + b^2} + \frac{ab}{a^2 + b^2}x - \frac{ab}{a^2 + b^2}x - \frac{b^2}{a^2 + b^2}x^2 \\ &= \frac{a^2}{a^2 + b^2} - \frac{b^2}{a^2 + b^2}x^2\end{aligned}$$
But since $-x^2 + I = 1 + I$ in this ring,
$$\left(\frac{a^2}{a^2 + b^2} - \frac{b^2}{a^2 + b^2}x^2\right) + I = \left(\frac{a^2 + b^2}{a^2 + b^2}\right) + I = 1 + I$$
.
(3) This is not even a domain! $x + I \neq 0 + I$, but $(x + I)(x + I) = x^2 + I = 0 + I$.
(4) Suppose that $f(x) + I = g(x) + I$.
(5)
(6) The kernel of φ is $0 + I$, so φ is

E: THE EVALUATION MAP Fix any real number a. Consider the evaluation map

$$\eta : \mathbb{R}[x] \to \mathbb{R} \qquad f \mapsto f(a)$$

(1) Understand why the evaluation map is a **surjective ring homomorphism.**
(2) Prove[1] that the kernel of η is the ideal $I = (x-a)$ of $\mathbb{R}[x]$ generated by $x-a$.
(3) Give a direct proof that $\mathbb{R}[x]/(x-a) \cong \mathbb{R}$ by thinking about the congruence classes $f + (x-a)$.[2] Why is there a bijection with $\mathbb{R}$ that preserves the ring structure?
(4) We say that a proper ideal[3] I in a ring R is **maximal** if whenever $I \subsetneq J$ for some ideal J, we have $J = R$. You will show on this week's homework that an ideal I in a commutative ring R is a maximal ideal if and only if R/I is a field.
Conclude that $(x-a)$ is maximal in $\mathbb{R}[x]$ for all a.
(5) Are there maximal ideals in $\mathbb{R}[x]$ that are not of the form $(x-a)$ for some $a \in \mathbb{R}$?

Solution.

(1) For any $\lambda \in \mathbb{R}$, the constant polynomial λ is taken to λ. This is a ring homomorphism because $1 \mapsto 1$, $\eta(f+g) = f(a) + g(a) = \eta(f) + \eta(g)$, and $\eta(fg) = f(a)g(a) = \eta(f)\eta(g)$.
(2) Elements in I are of the form $g(x)(x-a)$, and $\eta(g(x)(x-a)) = g(a)\cdot(a-a) = 0$. On the other hand, suppose $g \in \ker\eta$, and use the division algorithm to write $g(x) = h(x)(x-a) + r(x)$, where $r(x) = 0$ or has degree 0. Then $r(x) = r$ is a constant polynomial, and
$$0 = \eta\left(h(x)(x-a) + r(x)\right) = 0 + \eta(r(x)) = r.$$
Therefore, $g \in (x-a)$.
(3) We show that the map that takes $f(x)$ to its remainder when divided by $(x-a)$ is an isomorphism. The map is well-defined because the remainder is unique. The map is surjective because for all $r \in \mathbb{R}$, the constant polynomial r has remainder r. The map is injective because if $f(x)$ and $g(x)$ have the same remainder r, then $f(x) - q(x)(x-a) = g(x) - p(x)(x-a)$. Then $f(x) - g(x) = p(x)(x-a) - q(x)(x-a)$, so $(x-a)$ divides $f(x) - g(x)$. This means that $f(x)$ is congruent to $g(x)$ modulo $(x-a)$. (In this case, this is what it means to be injective). Finally, the map is a homomorphism because $1 + I$ maps to 1 and addition and multiplication work similarly to (1).
(4) Since we just showed that $\mathbb{R}[x]/(x-a) \cong \mathbb{R}$, which is a field, it must be that $(x-a)$ is maximal.
(5) There are! For example, we showed in part C that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, which is a field. Indeed, by B5, any ideal generated by a polynomial that is irreducible is maximal in $\mathbb{R}[x]$.

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

(1) Let $R = \mathbb{Z}[x]$ (recall that, since $\mathbb{Z}$ is not a field, we do not have unique factorization into irreducible polynomials!). Let I be the ideal $(5) \subset R$. Describe the quotient ring R/I.

[1] Hint for the harder direction: say $g \in \ker\eta$, and use the division algorithm to divide g by $x-a$; apply η.
[2] Hint: For quotient rings of polynomial rings over a field, every congruence class contains a unique [what?]
[3] A proper ideal is an ideal that is not equal to the whole ring R, i.e. I is a proper subset of the ring R.

(2) Let J be the ideal generated by $(5, f(x))$ in the quotient ring R/I, and let $\pi : R \longrightarrow R/I$ be the canonical homomorphism that maps x to $x + I$ for all $x \in R$. Show that

$$\pi(J) := \{\pi(j) | j \in J\}$$

is an ideal in R/I.

(3) Now let R be an arbitrary ring and I an arbitrary ideal of R. 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.

(4) 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.

(5) 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 $([7]_{42})$. (Note that we used that any ideal in $\mathbb{Z}$ is principal.)