MATH 315 Assignment 4

Instructor: Dr. Thomas Bitoun
Name: Yifeng Pan
UCID: 30063828

Winter 2020

Instructions

1. Any source MUST be cited. If you use somebody else's solution, you must demonstrate to the grader that you understand the proof you are using.
2. For each problem, you MUST indicate, along with your solution, the people you have been discussing the problem with. This includes the instructor and the TA. If you haven't discussed the problem with anyone, write so along with your solution, for each problem.
3. Write your solutions in your own words, and legibly. Please don't overcrowd your answers with unnecessary arguments.
4. Please submit your solutions as a portrait-oriented pdf and put your name in the filename.

With the exception of Problem (4.1), I completed every problem independently without discussion with anyone.

Sources are cited inline.

1 Let R be a commutative ring and let I and J be ideals of R.

1.1 Prove that the sets $I + J = \{x + y | x \in I, y \in J\}$, $I \cap J$ and $IJ = \{x_1y_1 + x_2y_2 + \ldots + x_ny_n | n \geq 1, x_m \in I, y_m \in J, \forall 1 \leq m \leq n\}$ are ideals of R.

1.1.1 [1] $I + J$:

Its clear that $I + J \neq \varnothing$.

Let $x + y, x' + y' \in I + J$. Now, $x+y+x'+y' = x+x'+y+y' \in I+J$.

Let $x + y \in I + J, r \in R$. Now, $r(x + y) = rx + ry \in I + J$.

Therefore $I + J$ is an ideal. □

1.1.2 $I \cap J$:

$\{0\} \subseteq I \cap J$.

Let $x, x' \in I \cap J$. Now, $x + x'$ is closed under I and under J, therefore $x + x' \in I \cap J$.

Let $x \in I + J, r \in R$. Now, $rx \in I$ and $rx \in J$,
therefore $rx \in I \cap J$.

Therefore $I \cap J$ is an ideal. □

1.1.3 IJ:

Its clear that $IJ \neq \varnothing$.

Let $z, z' \in IJ$. Now, $z + z' = x_1y_1 + \ldots + x_ny_n + x'_1y'_1 + \ldots + x'_{n'}y'_{n'} \in IJ$.

Let $z \in IJ, r \in R$. Now, $rz = r(x_1y_1 + \ldots + x_ny_n) = (rx_1)y_1 + \ldots + (rx_n)y_n$.
Since $\forall k, rx_k \in I$, so $rz \in IJ$.

Therefore IJ is a ideal. □

1.2 Show that $IJ \subset I \cap J$, and prove that if $I + J = R$, then $IJ = I \cap J$.

Let $z \in IJ$, where $z = x_1y_1 + x_2y_2 + \ldots + x_ny_n$, $x_k \in I, y_k \in J, \forall k$.

Since I is an ideal, we know $x_ky_k \in I$, $\forall k$. And since I is closed under addition, $z \in I$.

Simularly $z \in J$. Therefore $z \in I \cap J$, and $IJ \subseteq I \cap J$. □

Suppose $I + J = R$.

[2] $I \cap J = R(I \cap J) = (I + J)(I \cap J) = I(I \cap J) + J(I \cap J)$

Since $I \cap J \subseteq J$, we have $I(I \cap J) + J(I \cap J) \subseteq IJ + J(I \cap J) \subseteq IJ + JI = IJ$. □

Therefore $IJ = I \cap J$.

1.3 Let a and b be relatively prime integers. Prove that there are integers m, n such that $a^m + b^n = 1$ modulo ab. (i.e. $a^m + b^n = 1$ in $\mathbb{Z}/ab\mathbb{Z}$. Note that this makes sense for $ab < 0$ as well.)

[3] [4] By the Chinese Remainder Theorem: We define a ring isomorphism from $\mathbb{Z}/ab\mathbb{Z} \sim \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

It is sufficient to prove that $\exists m, n \in \mathbb{Z}$ such that $a^m + b^n \equiv 1 \pmod{a}$, and $a^m + b^n \equiv 1 \pmod{b}$.

Or equivalently: $b^n \equiv 1 \pmod{a}$, and $a^m \equiv 1 \pmod{b}$.

[5] By Euler's Theorem: Since a and b are coprimes, both m and n exists. □

[1] Reference: "Algebra" by Michael Artin, Section 11.3, Homomorphisms and Ideals.
[2] Reference: `https://en.wikipedia.org/wiki/Ideal_(ring_theory)#Ideal_operations`.
[3] Reference: `https://math.stackexchange.com/questions/901559/am-bn-equiv-1-mod-ab-for-some-m-n`.
[4] `https://en.wikipedia.org/wiki/Chinese_remainder_theorem#Theorem_statement`.
[5] `https://en.wikipedia.org/wiki/Euler's_theorem`

2 Let $a \in R$, where R is a commutative ring. Let $R[x]$ be the ring of polynomials over R.

2.1 Show that the factor ring $R[x]/(x-a)$, where $(x-a)$ is the principal ideal generated by $x-a \in R[x]$, is isomorphic to the ring R.

[6] Let $f : R[a] \to R$ be a ring homomorphism.

Since $(x-a)$ contains all multiples of $x-a$, we know $\forall i \in (x-a), f(i) = 0$. Now, suppose $i \notin (x-a)$. Then a is not a factor of i, and $f(i) \neq 0$. Therefore $(x-a) = \ker(f)$.

Now, Let $r \in R \subset R[x]$. Since $f(r) = r$, f is surjective.

Since f is surjective, and $(x-a) = \ker(f)$:
By the First Isomorphism Theorem, $\overline{f} : R[x]/(x-a) \to R$ is an isomorphism. □

2.2 Let $R' = R[x]/(ax-1)$ and let $u = [x]$ be the class of x in R'. Show that every element y of R' can be written as $y = u^l r$, where $l \geq 0$ and r is the class of a constant polynomial i.e. the class in R' of an element of R.

2.3 For which positive integers n does x^2+x+1 divide $x^4+3x^3+x^2+7x+5$ in the ring of polynomials over $\mathbb{Z}/n\mathbb{Z}$? Justify your answers.

We have $(x^2+x+1)(ax^2+bx+c) = (x^4+3x^3+x^2+7x+5)$ in $\mathbb{Z}/n\mathbb{Z}[x]$ for some $a, b, c \in \mathbb{Z}/n\mathbb{Z}$.

This gives

$$\begin{aligned}
a &\equiv 1 \pmod{n} \\
a+b &\equiv 3 \pmod{n} \\
a+b+c &\equiv 1 \pmod{n} \\
b+c &\equiv 7 \pmod{n} \\
c &\equiv 5 \pmod{n} \\
&\downarrow \\
a &\equiv 1 \pmod{n} \\
b &\equiv 2 \pmod{n} \\
c &\equiv 5 \pmod{n} \\
a+b+c &\equiv 1 \pmod{n} \\
&\downarrow \\
1+2+5 &\equiv 1 \pmod{n} \\
&\downarrow \\
7 &= kn \text{ for some } k, n \in \mathbb{Z}.
\end{aligned}$$

So $n \in \{1, 7\}$. □

[6] Reference: "Algebra" by Michael Artin, Section 11.4, Quotient Rings.

3

3.1 Prove that in the ring $\mathbb{Z}[x]$ of polynomials over the integers, the intersection of the principal ideals generated by 2 and x is the principal ideal generated by $2x$ i.e. $(x) \cap (2) = (2x)$.

(x) contains all the multiples of x. Or $(x) = \{zx | z \in Z[x]\}$.

(2) contains all the multiples of 2.

$(x) \cap (2)$ contians all multiples of 2 and x.

$(2x)$ contain all the multiples of $2x$.

$(x) \cap (2) = (2x)$. □

3.2 Which principal ideals of $\mathbb{Z}[x]$ are maximal ideals? Justify your answers.

[7] [8] Non.

Let $f(x) \in \mathbb{Z}[x]$ such that $(f(x))$ is a principal maximal ideal.

Suppose $f(x)$ is not a constant.

Since $2 \notin (f(x))$, we have $(f(x)) \subsetneq (f(x), 2)$.

Now, we need to prove $(f(x), 2) \neq \mathbb{Z}[x]$.

It is sufficient to prove $\forall a, b \in \mathbb{Z}[x], af(x) + 2b \neq 1$.

$af(x) + 2b = 1 \iff af(x)$ is an odd integer. But $f(x)$ is not a constant, so $af(x)$ cannot be a non-zero integer. We're done.

Now suppose $f(x) = c \neq 1$ is an integer. If $f(x) = 1$, then $(f(x))$ is not a maximal ideal.

Since $x \notin (c)$, we have $(c) \subsetneq (c, x)$.

It's analogous to verify that $1 \notin (c, k)$. We're done.

Therefore we can construct a proper ideal that is a strict superset of $(f(x))$ in both cases. And $(f(x))$ is not a maximal ideal. □

3.3 Let $\mathbb{R}$ be the field of real numbers. What are the maximal ideals of the factor ring $\mathbb{R}[x]/(x^2)$? Justify your answer.

Lemma: $\mathbb{R}[x]$ and $\mathbb{R}[x]/(x^2)$ are both principal ideal domains.

Let $\phi : \mathbb{R}[x] \to \mathbb{R}[x]/(x^2)$ be a surjective ring homomorphism, where $\ker \phi = (x^2)$.

The ideals of $\mathbb{R}[x]$ that contains (x^2) are (1), (x), and (x^2).

[9] By the Correspondence Theorem: The only ideals in $\mathbb{R}[x]/(x^2)$ are (1), $(x^2) = (0)$, and (x).

Therefore (x) is the only proper ideal, and the only maximal ideal. □

[7] Reference: Artin's Algebra, Section 11.8, Maximal Ideals.
[8] Reference: Third Example in `https://en.wikipedia.org/wiki/Maximal_ideal#Examples`.
[9] This is also stated in Artin's Algebra as Theorem 11.4.3:
`https://proofwiki.org/wiki/Correspondence_Theorem_for_Ring_Epimorphisms`

4 Let R be a commutative ring.

4.1 Assume that the characteristic of R is a prime number p. Prove that if $r \in R$ is nilpotent i.e. $r^n = 0$ for some $n \geq 0$, then there is an $l \geq 1$ such that $(1+r)^l = 1$.

Since the characteristic of R is p, $\forall r \in R, pr = 0$.

Let $r \in R$.

[10] We know $(1+r)^p = 1 + r^p$. And $(1+r)^{(p^k)} = 1 + r^{(p^k)}$.

[11] Choose k such that $p^k \geq n$.

Let $l = p^k$.

Then $(1+r)^l = 1 + r^l = 1 + r^n r^{l-n} = 1 + 0r^{l-n} = 1$. □

4.2 Prove that an integral domain of finite order is a field.

[12] Let $R = \{0, r_1, r_2, \ldots, r_{n-1}\}$ be an finite integral domain of order n.

We prove the only ideals of R are (0) and (1).

Let I be an ideal of R.

Suppose $I \neq (0)$.

Let $i \in I, i \neq 0$.

Let $J = (i) = \{ir | r \in R\} = \{0\} \cup \{ir_1, ir_2, \ldots, ir_{n-1}\}$.

We prove $ir_1, ir_2, \ldots, ir_{n-1}$ are distinct.

Suppose $\exists a, b, a \neq b$ such that $ir_a = ir_b$.

Now, $ir_a = ir_b \to 0 = ir_a - ir_b = i(r_a - r_b)$.

Since R is an integral domain, and $i \neq 0$, we know $r_a - r_b = 0$. Contradiction.

Therefore $ir_1, ir_2, \ldots, ir_{n-1}$ are distinct, and the order of J is $1 + (n-1) = n$.

Therefore $I = J = R$.

Therefore R only has two ideals.

[13] Therefore R is a field. □

4.3 Find $x \in \mathbb{Z}$ such that $x = 3$ modulo 8 and $x = 2$ modulo 5.

[14] 5 and 8 are coprimes.

So we only have to check integers between 0 and $5 * 8 = 45$.

The solutions to $x \equiv 2 \pmod 5$ are $\{2, 7, 12, 17, 22, 27, 32, 37, 42\}$.

The solutions to $x \equiv 3 \pmod 8$ are $\{3, 11, 19, 27, \ldots\}$.

We found $x = 27$.

Additional Citations

Proofread by Devin Kwok (UCID: 10016484).

[10] `https://en.wikipedia.org/wiki/Freshman%27s_dream#Prime_characteristic`.
[11] I got the idea that I needed $p^k \geq n$, not $p^k \equiv 0 \pmod n$, from Devin Kwok (UCID: 10016484).
[12] Reference: `https://en.wikipedia.org/wiki/Integral_domain`.
[13] Reference: "Algebra" by Michael Artin, Proposition 11.3.19 (b).
[14] Reference: `https://en.wikipedia.org/wiki/Chinese_remainder_theorem#Computation`.