Math 110A Homework 8

Jiaping Zeng

3/7/2021

1. Let R be an ring with identity and let I be an ideal of R.

   (a) If $1_R \in I$, prove that $I = R$.

   Answer: Take any $r \in R$, we must have $1_R \cdot r = r \in I$ by definition of ideal. Therefore every element of R is in I, so $I = R$.

   (b) If I contains a unit, prove that $I = R$.

   Answer: Let $a \in I$ be a unit, then by definition $ax = 1_R$ has a solution in R. Then by definition of ideal we have $ax = 1_R \in I$, therefore $I = R$ by part (a).

   (c) If I is an ideal in a field F, prove that either $I = (0_F)$ or $I = F$.

   Answer: By definition of field, $1_F \neq 0_F$. Then, if $1_F \in I$, we have $I = F$ by part (a); if not, we can only have $I = (0_F)$ or else we would again have $I = F$ by part (b) since every nonzero element is a unit.

2. Let I and J be ideals in R.

   (a) Prove that the set $K = \{a + b \mid a \in I, b \in J\}$ is an ideal in R that contains both I and J. K is called the **sum** of I and J, and is denoted $I + J$.

   Answer: Take $a, b \in I$ and $c, d \in J$, then $a + c \in K$ and $b + d \in K$. We have $(a + c) - (b + d) = (a - b) + (c - d) \in K$ since $a - b \in I$ and $c - d \in J$ by Theorem 6.1. We also have $r(a + c) \in K$ and $(a + c) \in K$ since $r(a + c) = ra + rc$ and $(a + c)r = ar + cr$, where $ra, ar \in I$ and $rc, cr \in J$ by Theorem 6.1. Then K satisfies both conditions of Theorem 6.1 and is therefore an ideal. It also contains both I and J upon taking $b = 0$ or $a = 0$ respectively in the definition.

   (b) Is the set $K = \{ab \mid a \in I, b \in J\}$ always an ideal in R?

   Answer: No; take $R = \mathbb{Z}$, $I = 2\mathbb{Z}$ and $J = 3\mathbb{Z}$. We have $4 \in I \subset K$ and $9 \in J \subset K$, so by Theorem 6.1 we must have $9 - 4 = 5 \in IJ$ which is not true.

   (c) Let IJ denote the set of all possible finite sums of elements of the form ab (with $a \in I, b \in J$), that is:

   $$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid n \geq 1, a_k \in I, b_k \in J\}.$$

   Prove that IJ is an ideal of R. IJ is called the **product** of I and J.

   Answer: Take $p, q \in IJ$ with $p = a_1b_1 + a_2b_2 + \cdots + a_nb_n$ and $q = c_1d_1 + c_2d_2 + \cdots + c_nd_n$, we have $p - q = a_1b_1 + a_2b_2 + \cdots + a_nb_n - c_1d_1 - c_2d_2 - \cdots - c_nd_n$ which is in IJ since each

$a_k b_k$ and $-c_k d_k$ is in IJ. Now take $r \in R$, we have $rp = r(a_1b_1 + a_2b_2 + \cdots + a_nb_n) = (ra_1)b_1 + (ra_2)b_2 + \cdots + (ra_n)b_n$. Since $ra_k \in I$ by Theorem 6.1 and $b_k \in J$, $rp \in IJ$. Similarly $pr \in IJ$ since $pr = (a_1b_1 + a_2b_2 + \cdots + a_nb_n)r = a_1(b_1r) + a_2(b_2r) + \cdots + a_n(b_nr)$. Therefore IJ is an ideal by Theorem 6.1.

3. Let R be an integral domain and $a, b \in R$. Show that $(a) = (b)$ if and only if $a = bu$ for some unit $u \in R$.

   Answer:

   $\Rightarrow$: Since $(a) = (b)$, we can take $ra = rb \cdot 1_R$ for every element of (a) and (b) (1_R always exists since R is an integral domain), then we have $a = bu$ with $u = 1_R$.

   $\Leftarrow$: Since $a = bu$, every element of (b) is a multiple of a in R. Then by definition of principal ideal (Theorem 6.2) $(a) = (b)$.

4. Let R be a commutative ring with $1_R \neq 0_R$, whose only ideals are (0) and R. Prove that R is a field.

   Answer: Take $a \in R$ where $a \neq 0$, then since $r \neq 0 \implies (a) \neq (0)$ we have $(a) = R$. Therefore $1_R \in (a)$ and by definition of ideal there exists some $r \in R$ such that $ar = 1_R$. Therefore we can always take $x = r$ as the solution to $ax = 1_R$, so R is a field.

5. Let I and K be ideals in a ring R, with $K \subseteq I$. Prove that $I/K = \{a + K \mid a \in I\}$ is an ideal in the quotient ring R/K.

   Answer: Take $a + K, b + K \in I/K$, we have $(a + K) - (b + K) = (a - b) + K \in I/K$. Now take $r + K \in R/K$, we have $(a + K)(r + K) = ar + K \in I/K$ and $(r + K)(a + K) = ra + K \in I/K$. Therefore I/K is an ideal by Theorem 6.1.

6. <u>*The Third Isomorphism Theorem*</u>: Let R be a ring, and let $I, K \subseteq R$ be ideals with $K \subseteq I$. By problem 5, I/K is an ideal of R/K. Prove that $(R/K)/(I/K) \approxeq R/I$.

   Answer: Take $f : R/K \to R/I, f(r + K) = r + I$. We have

$$f((a + K) + (b + K) = f((a + b) + K) = (a + b) + I = (a + I) + (b + I) = f(a + K) + f(b + K)$$

   and

$$f((a + K)(b + K)) = f(ab + K) = ab + I = (a + I)(b + I) = f(a + K)f(b + K).$$

   Therefore f is a homomorphism. It is also surjective since for every $r+I \in R/I$ we can take $r+K \in R/K$ such that $f(r + K) = r + I$. Note that the kernel of f is I/K since $f(r + K) = I \implies r \in I$ and $r + K \in I/K \implies r \in I \implies f(r + K) = r + I = I$. Then by the First Isomorphism Theorem $(R/K)/(I/K) \approxeq R/I$.

7. <u>*The Chinese Remainder Theorem*</u>: Let $m, n \in \mathbb{Z}$ be two *relatively prime* positive intgers.

   (a) Show that the function $f : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ defined by $f(x) = ([x]_m, [x]_n)$ is a homomorphism.

Answer: We have

$$f(a+b) = ([a+b]_m, [a+b]_n) = ([a]_m, [a]_n) + ([b]_m, [b]_n) = f(a) + f(b)$$

and

$$f(ab) = ([ab]_m, [ab]_n) = ([a]_m, [a]_n)([b]_m, [b]_n) = f(a)f(b).$$

Therefore f is a homomorphism.

(b) Show that $\ker f = mn\mathbb{Z}$.

Answer: Take $mnk \in mn\mathbb{Z}$, we have $f(mnk) = ([mnk]_m, [mnk]_n) = ([0]_m, [0]_n)$ since $mnk \equiv 0 \pmod{m}$ and $mnk \equiv 0 \pmod{n}$, so $mn\mathbb{Z} \subseteq \ker f$. Now take $a \in \mathbb{Z}$ such that $f(a) = ([0]_m, [0]_n)$, we must have $a \equiv 0 \pmod{m}$ and $a \equiv 0 \pmod{n}$, i.e. $m|a$ and $n|a$. Then $mn|a$, so $a \in mn\mathbb{Z}$ and $\ker f \subseteq mn\mathbb{Z}$. Therefore $\ker f = mn\mathbb{Z}$.

(c) Use the first isomorphism theorem to show that $\mathbb{Z}/mn\mathbb{Z} \approxeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

Answer: f is surjective since for every $([x]_m, [x]_n) \in (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ we always have $x \in \mathbb{Z}$. By part (a) f is a homomorphism, so f is a surjective homomorphism of rings. By part (b) $\ker f = mn\mathbb{Z}$, so by the First Isomorphism Theorem the quotient ring $\mathbb{Z}/mn\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

(d) Use part (c) to prove the Chinese Remainder Theorem: If $m, n \in \mathbb{Z}$ are relatively prime, and $a, b \in \mathbb{Z}$ are any integers, then there is a *unique* congruence class $[x] \in \mathbb{Z}/mn\mathbb{Z}$ satisfying the system of congruences

$$x \equiv a (\text{mod } m)$$

$$x \equiv b (\text{mod } n).$$

(in other words, there is some integer x satisfying both of these congruences, and if x and x' both satisfy these congruences then $x \equiv x' \pmod{mn}$).

Answer: By part (c) we have $\mathbb{Z}/mn\mathbb{Z} \approxeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$, so there exists an $x \in \mathbb{Z}/mn\mathbb{Z}$ such that $x \equiv a \pmod{m}$ and $x \equiv a \pmod{n}$. In addition, since we have an isomorphism such x is unique, i.e. $x \equiv x'$ if x, x' both satisfy the congruences.

8. Let $f : R \to S$ be a surjective homomorphism of commutative rings. If J is a prime ideal in S and $I = \{r \in R \mid f(r) \in J\}$, prove that I is a prime ideal in R.

Answer: Since J is a prime ideal in S, $J \neq S$, so $S - J$ is not empty. Then for any $r \in R$ and $s \in S - J$ such that $f(r) = s$, we have $r \notin I$. So $R - I$ is also not empty and therefore $I \neq R$. Now, for $ab \in I$, we have $f(ab) = f(a)f(b) \in J$. By definition of prime ideal we must have either $f(a) \in J$ or $f(b) \in J$, therefore we must have either $a \in I$ or $b \in I$, so by definition of prime ideal I is a prime ideal.