

**Math 395**  
**Homework 2**  
**Due: 2/8/2024**

**Name:** Avinash Iyer

**Collaborators:** Nate Hall, Nora Manukyan, Gianluca Crescenzo

**Problem 1**

Let  $R$  be a ring with identity and  $I$  an ideal in  $R$ .

- (a) We will prove that if  $I$  contains a unit, then  $I = R$ .

Specifically, by the definition of a unit  $u$ , for all  $a \in R$ ,  $ua = au = u$ .

If  $u \in I$ , then by the definition of ideal,  $au \in I$  and  $ua \in I$  for all  $a \in R$ . Therefore,  $a \in I$  for all  $a \in R$ , meaning  $I = R$ .

- (b) Let  $F$  be a field. We will show that if  $I$  is an ideal in  $F$ , then  $I = \{0_F\}$  or  $I = F$ .

Clearly,  $I = \{0_F\}$  is an ideal —  $I$  is closed under subtraction, multiplication, and multiplication by elements of  $F$  (as for  $a \in F$ ,  $a \cdot 0_F = 0_F \cdot a = 0_F$ ).

Suppose that  $I$  contains at least one element,  $a$ , where  $a \neq 0_F$ . Then, since  $a \neq 0_F$ , there is a multiplicative identity for  $a$ ,  $1/a$  such that  $a \cdot 1/a = 1/a \cdot a = 1_F$ . Since  $I$  is an ideal, this means  $I$  contains  $a \cdot 1/a$  as  $I$  is closed under multiplication by elements of the ring.

Therefore,  $I$  contains a unit of  $F$  (namely,  $1_F$ ), meaning  $I = F$  by the result from (a).

**Problem 2**

Let  $I, J$  be ideals in ring  $R$ . Define  $I + J = \{i + j \mid i \in I, j \in J\}$ . This is referred to as the sum of the ideals.

- (a) We will prove that  $I + J$  is an ideal in  $R$  that contains  $I$  and  $J$ .

To start, since  $I$  and  $J$  are ideals in  $R$ ,  $I$  and  $J$  are each subrings of  $R$ , meaning both  $I$  and  $J$  contain  $0_R$ . Therefore, taking  $j = 0_R$ , we find that  $\{i + 0_R \mid i \in I\} \subseteq I + J$ , and similarly, taking  $i = 0_R$ , we find that  $\{0_R + j \mid j \in J\} \subseteq I + J$ . These sets are, respectively,  $I$  and  $J$ , meaning  $I$  and  $J$  are both subsets of  $I + J$ .

We will now show  $I + J$  is an ideal in  $R$ . First,  $I + J$  is non-empty since, as exhibited earlier, both  $I$  and  $J$  are subrings, meaning  $0_R \in I$  and  $0_R \in J$ , so  $0_R + 0_R = 0_R \in I + J$ . Let  $x, y \in I + J$ . Then,  $x = x_i + x_j$  and  $y = y_i + y_j$  for some  $x_i, y_i \in I$  and  $x_j, y_j \in J$ . Then,

$$\begin{aligned} x - y &= (x_i + x_j) - (y_i + y_j) \\ &= (x_i - y_i) + (x_j - y_j), \end{aligned}$$

which is an element of  $I + J$ . Similarly,

$$\begin{aligned} xy &= (x_i + x_j)(y_i + y_j) \\ &= (x_i y_i) + (x_j y_j + x_i y_j + x_j y_i). \end{aligned}$$

Since  $x_i y_i \in I$ , as  $I$  is a subring, and  $x_j y_j \in J$ , as  $J$  is a subring, as well as  $x_i y_j \in J$  and  $x_j y_i \in J$  as  $J$  is an ideal, we have that  $x_j y_j + x_i y_j + x_j y_i \in J$ , so  $xy \in I + J$ .

Finally, we will show that  $I + J$  is closed under multiplication by elements from  $R$ . Let  $r \in R$ ,  $a \in I + J$ . Then,  $a = a_i + a_j$  for  $a_i \in I$  and  $a_j \in J$ . So,

$$\begin{aligned} ra &= r(a_i + a_j) \\ &= ra_i + ra_j, \end{aligned}$$

and

$$\begin{aligned} ar &= (a_i + a_j)r \\ &= a_i r + a_j r, \end{aligned}$$

and since  $I$  and  $J$  are both ideals,  $ra_i, a_i r \in I$  and  $ra_j, a_j r \in J$ , so  $ar, ra \in I + J$ .

Therefore,  $I + J$  is an ideal that contains  $I$  and  $J$ .

- (b) Let  $a, b \in \mathbf{Z}$ . We will show that  $a\mathbf{Z} + b\mathbf{Z} = \gcd(a, b)\mathbf{Z}$ .

By Bezout's identity, it is the case that there are integers  $x$  and  $y$  such that  $xa + yb = \gcd(a, b)$ . Since  $xa \in a\mathbf{Z}$ , and  $yb \in b\mathbf{Z}$ , as  $a\mathbf{Z}$  and  $b\mathbf{Z}$  are ideals in  $\mathbf{Z}$ , it is the case that for any  $n \in \mathbf{Z}$ ,  $n(xa + yb) \in a\mathbf{Z} + b\mathbf{Z}$ . Therefore,  $\gcd(a, b)\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z}$ .

For any  $na + mb \in a\mathbf{Z} + b\mathbf{Z}$ , there exist  $k, \ell \in \mathbf{Z}$  such that  $na = k \gcd(a, b)$  and  $mb = \ell \gcd(a, b)$ , by definition of greatest common divisor. Therefore,  $na + mb = (k + \ell) \gcd(a, b) \in \gcd(a, b)\mathbf{Z}$ , so  $a\mathbf{Z} + b\mathbf{Z} \subseteq \gcd(a, b)\mathbf{Z}$ .

Since  $\gcd(a, b)\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z}$ , and  $a\mathbf{Z} + b\mathbf{Z} \subseteq \gcd(a, b)\mathbf{Z}$ , it is the case that  $a\mathbf{Z} + b\mathbf{Z} = \gcd(a, b)\mathbf{Z}$ .

- (c) We will prove that if  $\gcd(a, b) = 1$ , then  $a\mathbf{Z} \cap b\mathbf{Z} = ab\mathbf{Z}$ .

To start, since  $a$  divides all members of  $ab\mathbf{Z}$ ,  $ab\mathbf{Z} \subseteq a\mathbf{Z}$ , and since  $b$  divides all members of  $ab\mathbf{Z}$ ,  $ab\mathbf{Z} \subseteq b\mathbf{Z}$ , meaning  $ab\mathbf{Z} \subseteq a\mathbf{Z} \cap b\mathbf{Z}$ .

Let  $k \in a\mathbf{Z} \cap b\mathbf{Z}$ . Then,  $k$  is a common multiple of  $a$  and  $b$ . Therefore,  $k$  is an integer multiple of  $\text{lcm}(a, b)$ , or  $\frac{ab}{\gcd(a, b)}$ . Since  $\gcd(a, b) = 1$ ,  $k$  is an integer multiple of  $ab$ . Therefore,  $k \in ab\mathbf{Z}$ , meaning  $a\mathbf{Z} \cap b\mathbf{Z} \subseteq ab\mathbf{Z}$ .

Since  $ab\mathbf{Z} \subseteq a\mathbf{Z} \cap b\mathbf{Z}$ , and  $a\mathbf{Z} \cap b\mathbf{Z} \subseteq ab\mathbf{Z}$ , it is the case that  $ab\mathbf{Z} = a\mathbf{Z} \cap b\mathbf{Z}$ .

### Problem 3

Let  $p$  be a prime number and let  $T$  denote the set of rational numbers in reduced form whose denominators are not divisible by  $p$ .

- (a) We will prove that  $T$  is a ring by showing closure under addition, identity and inverse under addition, commutativity of addition, closure under multiplication, associativity under multiplication, and distribution of multiplication over addition.

Let  $\frac{a}{b}, \frac{c}{d} \in T$  denote such rational numbers in lowest terms that satisfy the condition that  $p$  does not divide  $b$  and  $d$ , meaning that  $p$  is not a prime factor of either  $b$  or  $d$ . Then,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

and since the prime factors of  $bd$  are precisely the prime factors multiplied by the prime factors of  $d$ , and  $p$  is not a prime factor of  $b$  or  $d$ ,  $p$  is not a prime factor of  $bd$ , meaning  $p$  does not divide  $bd$ . Therefore,  $T$  is closed under addition.

The additive identity in lowest terms in  $T$  is inherited from the rational numbers — namely, 0. Since  $p$  does not divide 0, it is the case that  $T$  contains the additive identity.

The additive inverse to  $\frac{a}{b} \in T$  is  $\frac{-a}{b} \in T$ ; since  $p$  does not divide  $b$  by definition, it is the case that  $\frac{-a}{b}$  satisfies the necessary condition for  $T$ .

Since addition under  $T$  is inherited from addition under the rational numbers, addition in  $T$  is commutative, meaning  $T$  is an abelian group under addition.

Let  $\frac{a}{b}, \frac{c}{d} \in T$ , meaning  $p$  does not divide  $b$  and  $p$  does not divide  $d$ . Then,

$$\left(\frac{a}{b}\right) \left(\frac{c}{d}\right) = \frac{ac}{bd},$$

so by the same logic as with addition,  $p$  does not divide  $bd$ , meaning  $T$  is closed under multiplication.

Since multiplication is associative and distributive under the rational numbers, and  $T$  inherits these properties, it is the case that multiplication is associative and distributes over the rational numbers.

Therefore,  $T$  satisfies the necessary requirements for a ring.

- (b) Let  $I$  be the set of elements in  $T$  such that the numerator is divisible by  $p$ . We will show that  $I$  is an ideal by showing that  $I$  is a subring and multiplication by any element of  $T$  yields an element of  $I$ .

Since  $0 \in I$ , as the rational number 0 is divisible by every number, it is the case that  $I$  is non-empty. Let  $\frac{a}{b}, \frac{c}{d} \in I$ . Then,  $a = pk$  and  $c = p\ell$  for some  $k$  and  $\ell$ . Thus,

$$\begin{aligned} \frac{a}{b} - \frac{c}{d} &= \frac{pk}{b} - \frac{p\ell}{d} \\ &= \frac{pkd - p\ell b}{bd} \\ &= \frac{p(kd - \ell b)}{bd}, \end{aligned}$$

meaning that  $I$  is closed under subtraction. Similarly,

$$\begin{aligned} \left(\frac{a}{b}\right) \left(\frac{c}{d}\right) &= \frac{(pk)(p\ell)}{bd} \\ &= \frac{p(pk\ell)}{bd}, \end{aligned}$$

meaning  $I$  is closed under multiplication.

- (c) We will show that  $T/I$  has  $p$  distinct cosets.

By the definition of the equivalence relation of ideals,

$$\frac{a}{b} \sim \frac{c}{d}$$

if

$$\frac{a}{b} - \frac{c}{d} \in I.$$

Therefore,  $\frac{ad-bc}{bd} \in I$ , so  $p|ad-bc$ , so  $ad-bc \equiv 0$  modulo  $p$ . Therefore,  $ad \equiv bc$  modulo  $p$ , or  $\frac{a}{b} \equiv \frac{c}{d}$  modulo  $p$ .

Since  $\frac{a}{b} \equiv k$  modulo  $p$  for some  $k \in \{0, \dots, p-1\}$  necessarily, the values that  $\frac{a}{b}$  is congruent to, modulo  $p$ , form the cosets of  $T/I$ .

- (d) Let  $\varphi : T/I \rightarrow \mathbf{Z}/p\mathbf{Z}$  be defined as  $\varphi\left(\frac{a}{b}\right) = \left[\frac{a}{b}\right]_p$ . We will show that  $\varphi$  is an isomorphism.

Let  $\left[\frac{a}{b}\right]_{T/I} = \left[\frac{c}{d}\right]_{T/I}$ . Then,  $ad-bc \equiv 0$  modulo  $p$ . Applying  $\varphi$  to both sides, we get that  $\left[\frac{a}{b}\right]_p = \left[\frac{c}{d}\right]_p$ , meaning  $ad-bc \equiv 0$  modulo  $p$ . Therefore,  $\varphi$  is well-defined.

We will now show that  $\varphi$  is a ring homomorphism. Let  $\frac{a}{b}, \frac{c}{d} \in T/I$ . Then,

$$\varphi\left(\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)\right) = \left[\frac{a}{b}\frac{c}{d}\right]_p,$$

and by the properties of  $\mathbf{Z}/p\mathbf{Z}$ ,

$$\begin{aligned} &= \left[\frac{a}{b}\right]_p \left[\frac{c}{d}\right]_p \\ &= \varphi\left(\frac{a}{b}\right) \varphi\left(\frac{c}{d}\right). \end{aligned}$$

Similarly,

$$\varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \left[\frac{a}{b} + \frac{c}{d}\right]_p,$$

and by the properties of  $\mathbf{Z}/p\mathbf{Z}$ ,

$$\begin{aligned} &= \left[\frac{a}{b}\right]_p + \left[\frac{c}{d}\right]_p \\ &= \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right). \end{aligned}$$

Therefore,  $\varphi$  is a ring homomorphism.

We will now show that  $\varphi$  is a bijection. Clearly,  $\varphi$  is surjective, as we can select any  $\frac{a}{b} \in T/I$  such that  $\frac{a}{b} \in \mathbf{Z}/p\mathbf{Z}$ . To show that  $\varphi$  is injective, let  $\varphi\left(\frac{a}{b}\right) = \varphi\left(\frac{c}{d}\right)$ . Then,

$$\left[\frac{a}{b}\right]_p = \left[\frac{c}{d}\right]_p,$$

so

$$\frac{a}{b} \equiv \frac{c}{d} \text{ modulo } p.$$

Therefore, by the definition of equivalence modulo  $p$ ,

$$ad - bc \equiv 0 \text{ modulo } p,$$

so

$$\frac{a}{d} \sim_I \frac{c}{d}.$$

Since  $\varphi$  is a bijective ring homomorphism,  $\varphi$  is an isomorphism, meaning  $T/I \cong \mathbf{Z}/p\mathbf{Z}$ .

## Problem 5

Let  $\varphi : R \rightarrow S$  be a ring homomorphism. We will prove that  $\varphi$  is injective if and only if  $\ker \varphi = \{0_R\}$ .

In the forwards direction, we let  $\varphi$  be injective. Then,  $\varphi(0_R) = 0_S$  by the definition of a ring homomorphism. Since, for any  $a \in R, a \neq 0_R$ ,  $\varphi(a)$  cannot equal  $0_S$  (or else  $\varphi$  would not be injective), this means  $\ker \varphi = \{0_R\}$ .

In the reverse direction, we let  $\ker \varphi = \{0_R\}$ . Let  $\varphi(a) = \varphi(b)$ . Then,  $\varphi(a) - \varphi(b) = \varphi(b) - \varphi(b)$ , meaning  $\varphi(a) - \varphi(b) = 0_S$ . By the definition of a ring homomorphism, this is equivalent to  $\varphi(a - b) = 0_S$ . Since  $\ker \varphi = \{0_R\}$ , we have  $a - b = 0_R$ , or  $a = b$ . Thus,  $\varphi$  is injective.