

# Number Theory : Problem Set I

Youngduck Choi \*

## Abstract

This work contains solutions to some exercises in the problem set I.

### Question 1-1.

1. Let  $A$  be a ring. Show that an ideal  $\mathfrak{m} \subset A$  is maximal if and only if  $A/\mathfrak{m}$  is a field.

### Solution.

By proposition 1.1 in Atiyah-MacDonald, there is a one-to-one correspondence between the ideals of  $\mathfrak{b}$  of  $A$ , which contains  $\mathfrak{m}$ , and the ideals  $\bar{\mathfrak{b}}$  of  $A/\mathfrak{m}$ . Now, by proposition 1.2 in Atiyah-MacDonald,  $A/\mathfrak{m}$  is a field iff the only ideals of  $A/\mathfrak{m}$  are  $(0)$  and  $(1)$ , and by the one-to-one correspondence, the later is equivalent to  $\mathfrak{m}$  and  $A$  being the only ideals containing  $\mathfrak{m}$ , which is precisely definition of  $\mathfrak{m}$  being maximal.  $\square$

---

\*Department of Mathematics, Courant Institute of Mathematical Sciences, yc1104@nyu.edu; If you find an error and want to share with me, you can reach me via email.

**Question 1-2.**

2. Let  $A$  be a ring, and suppose that  $\mathfrak{m} \subset A$  is the unique maximal ideal of  $A$  (we say that  $A$  is a *local ring*). Show that an element  $a \in A$  is a unit if and only if  $a \notin \mathfrak{m}$ .

**Solution.**

Suppose  $a \in A$  is a unit. Then, there exists  $b \in A$ , such that  $ab = 1$ . If  $a \in \mathfrak{m}$ , then  $1 \in \mathfrak{m}$ , and  $\mathfrak{m} = A$ , which contradicts the fact that  $\mathfrak{m}$  is maximal, hence. Therefore,

$$a \text{ is a unit} \implies a \notin \mathfrak{m}.$$

From Atiyah-MacDonald, Corollary 1.5, which uses a standard Zorn's lemma argument, we know that every non-unit of  $A$  is contained in a maximal ideal. Therefore, by the uniqueness of  $\mathfrak{m}$  as a maximal ideal,

$$a \text{ is a non-unit} \implies a \in \mathfrak{m},$$

and hence, by contrapositive,

$$a \notin \mathfrak{m} \implies a \text{ is a unit},$$

which concludes

$$a \notin \mathfrak{m} \iff a \text{ is a unit},$$

as required. □

**Question 1-3.**

3. Give an example of a ring  $A$  and ideals  $\mathfrak{a}$  and  $\mathfrak{b}$  such that the set  $\{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$  is not an ideal.

**Solution.**

Consider  $A = \mathbb{R}[x, y]$ , and  $\mathfrak{a} = \mathfrak{b} = (x, y)$ . Then,  $x^2, y^2 \in \{ab : a \in \mathfrak{a}, b \in \mathfrak{b}\}$ , but  $x^2 + y^2 \notin \{ab : a \in \mathfrak{a}, b \in \mathfrak{b}\}$ .

**Question 1-4.**

4. Let  $A$  be an integral domain. Recall that for  $a \in A$ , the *principal ideal* defined by  $a$  is

$$(a) = \{ax \mid x \in A\}$$

Prove the following:

- (a) Two elements  $a, b \in A$  are associates if and only if  $(a) = (b)$ .
- (b) For any  $a, b \in A$ ,  $(ab) = (a)(b)$ .
- (c) For any  $a, b \in A$ ,  $a \mid b$  if and only if  $(b) \subset (a)$ .
- (d) For any  $a, b \in A$ ,  $(a) \subsetneq (b)$  if and only if there exists a principal ideal  $(c)$  such that  $(b) = (a)(c)$ .
- (e) An element  $a \in A$  is irreducible if and only if  $(a)$  is maximal among the principal ideals of  $A$ , in other words, if  $(a) \subset (b)$  implies  $(a) = (b)$ .
- (f) An element  $a \in A$  is prime if and only if  $(a)$  is a prime ideal.
- (g) An element  $a \in A$  is a unit if and only if  $(a)$  is the unit ideal.

**Solution.**

(a) Observe that  $a, b \in A$  are associates, there exists a unit  $c$  such that  $a = bc$  is equivalent to there exists  $c, d$  units such that  $a = bc$  and  $b = ad$ . To see this, if  $c$  is a unit and  $a = bc$ , then there exists  $d$  such that  $cd = 1$ , and multiplying both sides by  $d$  gives,  $ad = b$ , and by definition  $d$  is a unit.

Suppose  $a, b$  are associates. Then, if  $ax \in (a)$ , then set  $y = cx$ , so  $ax = bcx - by \in (b)$ . Therefore,  $(a) \subset (b)$  and similarly, by the above discussion  $(b) \subset (a)$  and hence  $(a) = (b)$ . Conversely, suppose that  $(a) = (b)$ . Then,  $a = bx$  for some  $x \in A$ , and  $b = ay$  for some  $y \in A$ . Therefore,  $a = ayx$ , so  $1 = yx$ . This shows that  $x$  is a unit, and  $a, b$  are associates.

(b)

**Question 1-5.**

5. Let  $[0, 1]$  denote the unit interval, and let  $C^0[0, 1]$  denote the ring of continuous real-valued functions on  $[0, 1]$ . For  $a \in [0, 1]$ , define

$$\mathfrak{m}_a = \{f \in C^0[0, 1] \mid f(a) = 0\}.$$

- (a) Show that  $\mathfrak{m}_a$  is a maximal ideal of  $C^0[0, 1]$ .  
(b) Show that any maximal ideal of  $C^0[0, 1]$  is equal to  $\mathfrak{m}_a$  for some  $a \in [0, 1]$ .

**Solution.**

We prove the statements in a slightly more general setting. Let  $X$  be compact and Hausdorff space, and  $C(X)$  be the ring of all real-valued continuous functions on  $X$ . For each  $x \in X$ , let  $\mathfrak{m}_x$  be the set of all  $f \in C(X)$  such that  $f(x) = 0$ .

- (a) Now, for any  $x \in X$ , we know that  $\text{eval}_x : C(X) \rightarrow \mathbb{R}$ , defined by

$$\text{eval}_x(f) \mapsto f(x) \quad (f \in C(X))$$

is a surjective ring-homomorphism. Then,  $\mathfrak{m}_x$  can be viewed as a kernel of  $\text{eval}_x$ , so  $\mathfrak{m}_x$  is maximal.

- (b) Now, with (a) established, we can view  $x \mapsto \mathfrak{m}_x$  as a map from  $X$  to  $\text{Max}(C(X))$ , where the latter denotes the set of all maximal ideals of  $C(X)$ . We denote this map as  $\mu$ . Then, (b) asserts that  $\mu$  is surjective, which we show now. Let  $\mathfrak{m}$  be any maximal ideal in  $C(X)$ . Set

$$V = \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}.$$

Suppose  $V$  is empty. Then, for each  $x \in X$ , we can find  $f_x \in \mathfrak{m}$  such that  $f_x(x) \neq 0$ . By continuity of  $\{f_x\}_{x \in X}$ , we can choose an open cover of  $X$ ,  $\{U_x\}_{x \in X}$ , such that  $f_x(U_x) \cap \{0\} = \emptyset$  for all  $x \in X$ . Now, by compactness, there exists a sub-cover of the cover  $\{U_i\}_{i \leq n}$ . Now, set

$$f = \sum_{i \leq n} f_i^2,$$

where  $f_i$ s are the corresponding functions in  $\mathfrak{m}$  for  $U_i$ s in the construction. Then,  $f \in \mathfrak{m}$  does not vanish anywhere, so it is a unit, which contradicts the fact that  $\mathfrak{m}$  is a maximal ideal. Hence,  $V$  is non-empty, so  $x_0 \in V$  for some  $x_0 \in X$ . Then,  $\mathfrak{m} \subset \mathfrak{m}_{x_0}$ , and by maximality of  $\mathfrak{m}$  and  $\mathfrak{m}_{x_0}$ , we see that  $\mathfrak{m} = \mathfrak{m}_{x_0}$ . In other words,  $\mathfrak{m} = \mu(x_0)$ . Therefore,  $\mu$  is surjective and, we are done.  $\square$