

# Exercises from Ch 2: Rings, Lang

Matthew Gergley

Last Updated: November 24, 2025

## Exercises

**Exercise 0.1.** (Exercise 2) Let  $f: A \rightarrow A'$  be a surjective homomorphism of rings, and assume that  $A$  is local,  $A \neq 0$ . Show that  $A'$  is local.

*Proof.* Since  $A$  is local by assumption, there exists a unique ideal  $\mathfrak{m} \subseteq A$  such that  $A/\mathfrak{m}$  is a field. Define  $\mathfrak{m}' = f(\mathfrak{m}) = \{f(x) : x \in \mathfrak{m}\} \subseteq A'$ . Let  $f_*: A/\mathfrak{m} \rightarrow A'/\mathfrak{m}'$  be given by  $f_*(a\mathfrak{m}) = f(a)\mathfrak{m}'$ . We proceed by showing that  $A'/\mathfrak{m}'$  is a field and thus we begin by showing that  $\mathfrak{m}' \subseteq A'$  is an ideal. Since  $A \neq 0$  which implies that  $\mathfrak{m} \neq 0$ , we know that  $\mathfrak{m}' \neq 0$  and that  $\mathfrak{m}' \subseteq A'$  since  $f$  is a surjection. Let  $x_1, x_2 \in \mathfrak{m}'$ . Then, there exists  $a, b \in \mathfrak{m}$  such that  $x_1 = f(a)$  and  $x_2 = f(b)$ . Hence,  $x_1 - x_2 = f(a) - f(b) = f(a - b) \in \mathfrak{m}'$  since  $a - b \in \mathfrak{m}$ .

Next,  $x_1 x_2 = f(a)f(b) = f(ab) \in \mathfrak{m}'$  since  $ab \in \mathfrak{m}$ . Therefore,  $\mathfrak{m}' \subseteq A'$  is a subring. Now let  $\alpha = f(a) \in A'$  and  $\beta = f(x) \in \mathfrak{m}'$ . Then,  $\alpha\beta = f(a)f(x) = f(ax) \in \mathfrak{m}'$  since  $ax \in \mathfrak{m}$ . Also,  $\beta\alpha \in \mathfrak{m}'$  from the commutativity of  $A$  (since it is local). Thus,  $\mathfrak{m}' \subseteq A'$  is an ideal.

We now proceed by showing that  $A'/\mathfrak{m}'$  is a field if and only if  $\mathfrak{m}'$  is maximal.

( $A'/\mathfrak{m}'$  is a commutative ring) By definition, we first show that  $(A'/\mathfrak{m}', +)$  is a commutative group. Note that most deductions will come from the fact that  $A'$  is a ring. First,  $A'/\mathfrak{m}' \neq 0$  since the identity in  $A'/\mathfrak{m}'$  is  $f(0)\mathfrak{m}' = 0\mathfrak{m}' = 0$ . Let  $a\mathfrak{m}', b\mathfrak{m}', c\mathfrak{m}' \in A'/\mathfrak{m}'$ , then

$$\begin{aligned} a\mathfrak{m}' + (b\mathfrak{m}' + c\mathfrak{m}') &= a\mathfrak{m}' + (b + c)\mathfrak{m}' \\ &= (a + b + c)\mathfrak{m}' \\ &= (a + b)\mathfrak{m}' + c\mathfrak{m}' \\ &= (a\mathfrak{m}' + b\mathfrak{m}') + c\mathfrak{m}' \end{aligned}$$

Let  $a\mathfrak{m}' \in A'/\mathfrak{m}'$ . Because  $A'$  is a ring, there exists  $a^{-1} \in (A', +)$  such that  $f(x) = a^{-1}$  for some  $x \in A$  and such that  $a\mathfrak{m}' + a^{-1}\mathfrak{m}' = 0\mathfrak{m}' = 0$ . Finally,  $(A'/\mathfrak{m}', +)$  is closed by the fact that  $(A', +)$  is a group. Hence,  $f(A)/f(\mathfrak{m}) = A'/\mathfrak{m}'$  is an additive abelian group.

Define multiplication of cosets in the usual way. Associativity for multiplication in  $A'/\mathfrak{m}'$  follows from associativity of  $(A', \cdot)$ .

(Distributivity) Let  $x\mathfrak{m}', y\mathfrak{m}', z\mathfrak{m}' \in A'/\mathfrak{m}'$ . Then,

$$\begin{aligned} (x\mathfrak{m}' + y\mathfrak{m}')z\mathfrak{m}' &= ((x + y)\mathfrak{m}')(z\mathfrak{m}') \\ &= (xz + yz)\mathfrak{m}' \\ &= xz\mathfrak{m}' + yz\mathfrak{m}' \end{aligned}$$

Likewise,  $z\mathfrak{m}'(x\mathfrak{m}' + y\mathfrak{m}') = zx\mathfrak{m}' + zy\mathfrak{m}'$ . Therefore,  $A'/\mathfrak{m}'$  is a ring. Furthermore, it is commutative since if  $a\mathfrak{m}' = f(x)\mathfrak{m}', b\mathfrak{m}' = f(y)\mathfrak{m}' \in A'/\mathfrak{m}'$ , then  $(a\mathfrak{m}')(b\mathfrak{m}') = ab\mathfrak{m}' = f(x)f(y)\mathfrak{m}' = f(xy)\mathfrak{m}' = f(yx)\mathfrak{m}' = f(y)f(x)\mathfrak{m}' = ba\mathfrak{m}' = (b\mathfrak{m}')(a\mathfrak{m}')$ . Since  $A/\mathfrak{m}$  is a field, for all  $x\mathfrak{m} \in A/\mathfrak{m}$ , there exists  $(x\mathfrak{m})^{-1} = x^{-1}\mathfrak{m} \in A/\mathfrak{m}$  such that  $(x\mathfrak{m})(x^{-1}\mathfrak{m}) = 1\mathfrak{m}$ . Then,  $f_*(x\mathfrak{m}) = f(x)\mathfrak{m}'$  and  $f_*(x^{-1}\mathfrak{m}) = f(x^{-1})\mathfrak{m}' = f(x)^{-1}\mathfrak{m}'$ . Hence, for all  $x'\mathfrak{m}' \in A'/\mathfrak{m}'$ , there exists  $(x'\mathfrak{m}')^{-1} \in A'/\mathfrak{m}'$  by the surjectivity of  $f$ . Therefore,  $A'/\mathfrak{m}'$  is a field if and only if  $\mathfrak{m}' \subseteq A' = f(A)$  is maximal. Now, we must show that if  $\mathfrak{n} \subseteq A'$  is another maximal ideal, then  $\mathfrak{m}' = \mathfrak{n}$ . This follows trivially by reversing the inclusion of  $\mathfrak{m}' \subseteq \mathfrak{n}$  and  $\mathfrak{n} \subseteq \mathfrak{m}'$  by the maximality of either ideal. Thus,  $\mathfrak{m}'$  is a unique maximal ideal of  $A'$  and therefore  $A'$  is local.

**MAYBE CHECK THE ZERO DIVISORS IN THE QUOTIENT RING!!!!!!!**

□

**Exercise 0.2.** (Exercise 4) Let  $A$  be a principal ring and  $S$  a multiplicative subset with  $0 \notin S$ . Show that  $S^{-1}A$  is principal.

*Proof.* Define  $f : A \rightarrow S^{-1}A$  be given by the canonical localization map  $f(a) = a/1$ . Let  $J \subseteq S^{-1}A$  be an ideal and define

$$I = f^{-1}(J) = \{x \in A : x/1 \in J\} \subseteq A.$$

Case 1: ( $I \cap S \neq \emptyset$ ) Let  $s \in I \cap S \Rightarrow s/1 \in J$ . By definition of localization,  $s/1$  is a unit in  $S^{-1}A$  with  $(s/1)^{-1} = 1/s$ . Hence, since  $J$  is an ideal that contains a unit  $\underbrace{(s/1)}_{\in J} \underbrace{(1/s)}_{\in S^{-1}A} = 1/1 = 1 \in J$ . But if

$1 \in J$ , then  $J = S^{-1}A$ . Hence,  $J$  is principal with  $J = S^{-1}A = (1/1) = (1)$ .

Case 2: ( $I \cap S = \emptyset$ ) WTS  $J = S^{-1}I$ . ( $\subseteq$ ) If  $x/s \in J$ , then  $x/1 = (x/s)(s/1) \in J \Rightarrow x \in I$ . Hence,  $x/s \in S^{-1}I$  and thus  $J \subseteq S^{-1}I$ . ( $\supseteq$ ) If  $x \in I$ , then  $x/1 \in J$ . Since  $J$  is an ideal, for all  $s \in S$ , we have

$$\underbrace{(x/1)}_{\in J} \underbrace{(1/s)}_{\in S^{-1}A} = x/s \in J.$$

Thus,  $J \supseteq S^{-1}I$ . Finally, since  $A$  is principal,  $I = (a)$ . Therefore,  $J = S^{-1}I = S^{-1}(a) = (a/1)$ . Hence,  $J$  is principal generated by  $a/1$ . Therefore, every ideal  $J \subseteq S^{-1}A$  is principal and thus  $S^{-1}A$  is principal.  $\square$

**Exercise 0.3.** (Exercise 6) Let  $A$  be a factorial ring and  $p$  a prime element. Show that the local ring  $A_{(p)}$  is principal.

*Proof.* If  $A$  is also principal, then we are done by Exercise 4. Thus, suppose  $A$  is only factorial. Let  $p$  be an irreducible (prime) element of  $A$ . Thus,  $(p) \subseteq A$  is a prime ideal. Set  $S = A \setminus (p)$ . Hence,

$$S^{-1}A = A_{(p)} = \{x/s : x \in A, s \notin (p)\}.$$

Let  $\mathfrak{m} := \{x/s \in A_{(p)} : x \in (p)\}$ . By definition, if  $x \notin (p)$ , then  $x \in S$ , so  $x/1$  is invertible in the localization (since  $1 \in A$ ,  $x \in S$ ,  $1/x \in A_{(p)}$ ). Thus,  $x/s$  is invertible. Now, if  $x \in (p)$ , then no matter what  $y/t \in A_{(p)}$  we multiply by, we obtain  $xy/st \in (p)A_{(p)} = \{pa/s : a \in A, s \notin (p)\} = (p/1) \subseteq A_{(p)}$ , which is never equal to 1. Thus, it is not invertible, so  $A \setminus \mathfrak{m} = A_{(p)}^\times$  (units of  $A_{(p)}$ ). Thus,  $A_{(p)}/\mathfrak{m}$  is a field. Therefore,  $\mathfrak{m}$  is the unique maximal ideal of  $A_{(p)}$ , hence  $A_{(p)}$  is local.

Finally, if  $x \in (p)$ , we write  $x = pk$ . Then

$$x/s = (p/1) \cdot (k/s),$$

so every element of  $\mathfrak{m}$  is a multiple of  $p/1$ . Thus,  $\mathfrak{m} = (p/1)$ .

Now we must show all ideals are principal. Let  $I$  be a nonzero ideal of  $A_{(p)}$ . Pick an element  $x/s \in I$  with  $x \neq 0$  having the smallest exponent of  $p$  in its factorization  $x = up^n$  (where  $u$  is a unit in  $A$ ). Then

$$x/s = (p/1)^n \cdot (u/s),$$

and  $u/s$  is a unit in  $A_{(p)}$ , since  $u \notin (p)$ . Hence  $(x/s) = (p/1)^n$ . If  $y/t \in I$ , then  $y = u'p^m$  for some  $m \geq n$  by minimality of  $n$ , and thus

$$y/t = (p/1)^m \cdot (u'/t) \in (p/1)^n.$$

Therefore  $I = (p/1)^n$ , proving that every ideal of  $A_{(p)}$  is principal.

Thus,  $A_{(p)}$  is principal.  $\square$

## Dedekind rings

Prove the following statements about a Dedekind ring  $\mathfrak{o}$ . To simplify terminology, by an **ideal** we shall mean non-zero ideal unless otherwise specified. We let  $K$  denote the quotient field of  $\mathfrak{o}$ .

**Exercise 0.4.** (Exercise 17)

As for the integers, we say that  $\mathfrak{a} \mid \mathfrak{b}$  ( $\mathfrak{a}$  **divides**  $\mathfrak{b}$ ) if there exists an ideal  $\mathfrak{c}$  such that  $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ . Prove:

a)  $\mathfrak{a} \mid \mathfrak{b}$  if and only if  $\mathfrak{b} \subseteq \mathfrak{a}$ .

b) Let  $\mathfrak{a}, \mathfrak{b}$  be ideals. Then  $\mathfrak{a} + \mathfrak{b}$  is their greatest common divisor. In particular,  $\mathfrak{a}, \mathfrak{b}$  are relatively prime if and only if  $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ .

*Proof.* a) Note that  $\mathfrak{a}, \mathfrak{b}$  are non-zero ideals of the Dedekind ring  $\mathfrak{o}$ .

( $\Rightarrow$ ) Assume  $\mathfrak{a} \mid \mathfrak{b}$ . By definition this means there exists an ideal  $\mathfrak{c}$  such that

$$\mathfrak{b} = \mathfrak{a}\mathfrak{c}.$$

Since  $\mathfrak{c} \subseteq \mathfrak{o}$ , we have  $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$ . Thus  $\mathfrak{b} \subseteq \mathfrak{a}$ .

( $\Leftarrow$ ) Conversely, assume  $\mathfrak{b} \subseteq \mathfrak{a}$ . Since  $\mathfrak{o}$  is Dedekind, every non-zero ideal has a unique factorization into prime ideals. Namely, write

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_{\mathfrak{p}}} \quad \text{and} \quad \mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{\beta_{\mathfrak{p}}}$$

Observe that for all  $\mathfrak{p}$ , we have  $\mathfrak{p}^m \subseteq \mathfrak{p}^n$  if and only if  $m \geq n$ . Then  $\mathfrak{b} \subseteq \mathfrak{a} \Rightarrow \beta_{\mathfrak{p}} \geq \alpha_{\mathfrak{p}}$  for all  $\mathfrak{p}$ . Define another ideal,

$$\mathfrak{c} = \prod_{\mathfrak{p}} \mathfrak{p}^{\beta_{\mathfrak{p}} - \alpha_{\mathfrak{p}}}$$

Note that  $\beta_{\mathfrak{p}} - \alpha_{\mathfrak{p}} \geq 0$  for all  $\mathfrak{p}$  and thus  $\mathfrak{c} \subseteq \mathfrak{o}$  (since the product of ideals is an ideal). Then,

$$\mathfrak{a}\mathfrak{c} = \left( \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_{\mathfrak{p}}} \right) \left( \prod_{\mathfrak{p}} \mathfrak{p}^{\beta_{\mathfrak{p}} - \alpha_{\mathfrak{p}}} \right) = \prod_{\mathfrak{p}} \mathfrak{p}^{\beta_{\mathfrak{p}}} = \mathfrak{b}$$

Hence,  $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \Rightarrow \mathfrak{a} \mid \mathfrak{b}$ .

b) The G.C.D. of ideals is analogous to the definition of G.C.D. in the integers:

An ideal  $\mathfrak{d}$  is the  $\gcd(\mathfrak{a}, \mathfrak{b})$  if  $\mathfrak{d} \mid \mathfrak{a}$  and  $\mathfrak{d} \mid \mathfrak{b}$ ; if  $\mathfrak{c}$  is any ideal such that  $\mathfrak{c} \mid \mathfrak{a}$  and  $\mathfrak{c} \mid \mathfrak{b}$ , then  $\mathfrak{c} \mid \mathfrak{d}$ .

We claim that  $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ .

We have  $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$  and  $\mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$ . Therefore, by part (a),  $\mathfrak{a} + \mathfrak{b} \mid \mathfrak{a}$  and  $\mathfrak{a} + \mathfrak{b} \mid \mathfrak{b}$ . Now suppose there exists an ideal  $\mathfrak{c}$  such that  $\mathfrak{c} \mid \mathfrak{a}$  and  $\mathfrak{c} \mid \mathfrak{b}$ . Then, again by part (a),  $\mathfrak{a} \subseteq \mathfrak{c}$  and  $\mathfrak{b} \subseteq \mathfrak{c}$ . We want to show  $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$ . But if  $z = x + y \in \mathfrak{a} + \mathfrak{b}$ , then  $x \in \mathfrak{a} \subseteq \mathfrak{c}$  and  $y \in \mathfrak{b} \subseteq \mathfrak{c}$ . Since ideals are closed under addition,  $z = x + y \in \mathfrak{c}$ . Hence,

$$\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$$

Then by utilizing part (a) again, we have  $\mathfrak{c} \mid \mathfrak{a} + \mathfrak{b}$ . Therefore,  $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b})$ .

The particular case mentioned follows immediately since if  $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$  (unit ideal, the whole Dedekind ring), then by what we have shown  $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ . The converse is clearly true as well. □

**Exercise 0.5.** (Exercise 19)

Let  $\mathfrak{a}, \mathfrak{b}$  be ideals of a Dedekind domain  $\mathfrak{o}$ . Show that there exists an element  $c \in K$  (the quotient field of  $\mathfrak{o}$ ) such that  $c\mathfrak{a}$  is an ideal relatively prime to  $\mathfrak{b}$ . In particular, every ideal class in  $\text{Pic}(\mathfrak{o})$  contains representative ideals prime to a given ideal.

*Proof.* □