Exercises from Ch 2: Rings, Lang

Matthew Gergley

Last Updated: January 9, 2026

Exercises

Exercise 0.1. (Exercise 1) Suppose that $1 \neq 0$ in A. Let S be a multiplicative subset of A not containing 0. Let $\mathfrak{p}$ be a maximal element in the set of ideals of A whose intersection with S is empty. Show that $\mathfrak{p}$ is prime.

Proof. Denote the set of ideals of A whose intersection with S is empty by

$$J(A) = \{I \subseteq A \text{ ideal}: \ I \cap S = \varnothing\}.$$

Let $\mathfrak{p} \in J(A)$ be maximal. Hence, for all $I \in J(A) \setminus \mathfrak{p}$, $I \subseteq \mathfrak{p}$. By definition, $\mathfrak{p} \cap S = \varnothing$. Let $a, b \in A$ such that $ab \in \mathfrak{p}$. If $a \in \mathfrak{p}$, we are done. Thus, assume $a \notin \mathfrak{p}$.
Case 1 ($a \in S$): By way of contradiction, suppose $b \notin \mathfrak{p}$. We form the ideal

$$\mathfrak{p} + (b) = \{x + rb: \ x \in \mathfrak{p}, \, r \in A\}.$$

Then, $\mathfrak{p} \subseteq \mathfrak{p} + (b)$. But $\mathfrak{p} + (b) \notin J(A)$ by the maximality of $\mathfrak{p} \in J(A)$. Thus,

$$(\mathfrak{p} + (b)) \cap S \neq \varnothing.$$

Then, there exists some $s \in S$ such that $s = x + rb$. Choose $r = a \in A$. Thus, $s = x + ab \in \mathfrak{p}$ since $x \in \mathfrak{p}$ and $ab \in \mathfrak{p}$ by assumption. Thus, $s \in \mathfrak{p}$. But $s \in S$ and $\mathfrak{p} \cap S = \varnothing$. Contradiction! Therefore, $b \in \mathfrak{p}$.
Case 2 ($a \notin S$): Hence, $a \notin \mathfrak{p}$ and $a \notin S$, thus $a \in A$ strictly. Consider the ideal

$$\mathfrak{p} + (a) = \{x + ra: \ x \in \mathfrak{p}, \, r \in A\}.$$

Then, since $a \notin \mathfrak{p}$, $\mathfrak{p} \subseteq \mathfrak{p} + (a)$. But $\mathfrak{p} + (a) \notin J(A)$ by the maximality of $\mathfrak{p} \in J(A)$. Thus,

$$(\mathfrak{p} + (a)) \cap S \neq \varnothing.$$

Then, there exists some $s \in S$ such that $s = x + ra$ with $r = b \notin \mathfrak{p}$. Thus, $x + ba \in \mathfrak{p} \Rightarrow s \in \mathfrak{p}$. but $s \in S$ and $\mathfrak{p} \cap S = \varnothing$. Contradiction! Thus, $b \in \mathfrak{p}$.

$\square$

Exercise 0.2. (Exercise 2) Let $f\colon A \to A'$ be a surjective homomorphism of rings, and assume that A is local, $A \neq 0$. Show that A' is local.

Proof. Since f is surjective, by the First Isomorphism Theorem, $A' \cong A/\ker f$. Let $\mathfrak{m} \subseteq A$ be the unique maximal ideal (since A is local by assumption). Since $A' \neq 0$, we have $\ker f \subsetneq A$ (proper ideal) which implies $\ker f \subseteq \mathfrak{m}$ since $\mathfrak{m}$ is maximal. Maximal ideals of the quotient ring $A/\ker f$ are in bijection with maximal ideals $\mathfrak{n} \subseteq A$ such that $\ker f \subseteq \mathfrak{n}$ via $\mathfrak{n} \mapsto \mathfrak{n}/\ker f$. Since A has exactly one maximal ideal $\mathfrak{m}$ and $\ker f \subseteq \mathfrak{m}$, it follows that $A/\ker f$ has exactly one maximal ideal $\mathfrak{m}/\ker f$. Define

$$\varphi\colon A/\ker f \to A'$$

by $\varphi(x + \ker f) = f(x)$ for all $x \in A$. Hence, $\varphi(\mathfrak{m}/\ker f) = \{f(x)\colon x \in \mathfrak{m}\} = f(\mathfrak{m})$. Therefore, under $A' \cong A/\ker f$, $\mathfrak{m}/\ker f$ corresponds to $f(\mathfrak{m}) \subseteq A'$, i.e. $\mathfrak{m}/\ker f$ and $f(\mathfrak{m})$ are the "same" ideal just in different "languages". Thus, A' has a unique maximal ideal (and commutative by assumption), A' is local.

$\square$

Exercise 0.3. (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 $f : A \to S^{-1}A$ 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: $(I \cap S \neq \varnothing)$ 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: $(I \cap S = \varnothing)$ 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. □

Exercise 0.4. (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. □

Exercise 0.5. (Exercise 7) Let A be a principal ring $a_1, \ldots, a_n$ non-zero elements of A. Let $(a_1, \ldots, a_n) = (d)$. Show that d is a greatest common divisor for the a_i $(i = 1, \ldots, n)$.

Proof. By construction, $a_i \in (a_1, \ldots, a_n) = (d)$ $\left(\text{i.e. } a_i = \sum_{i=1}^{n} x_i a_i, \text{ w/ } x_j = 0 \text{ if } j \neq i \text{ and } x_j = 1 \text{ if } j = i\right)$. Thus, there exists $b_i \in A$ such that $a_i = b_i d$ for all $1 \leq i \leq n$. Hence, $d \big| a_i$ for all $1 \leq i \leq n$. Now, suppose that there exists $c \in A$ such that $c \big| a_i$ for all $1 \leq i \leq n$. Then, for all i, there exists $y_i \in A$ such that $a_i = y_i c$. Therefore, $a_i \in (c)$ (since if $x_1 a_1 + \cdots + x_n a_n \in (a_1, \ldots, a_n)$, then by the above $x_1 y_1 c + \cdots + x_n y_n c \in (c)$, clearly). But by assumption, $(a_1, \ldots, a_n) = (d)$, whence $(d) \subseteq (c)$. Thus, there exists $z \in A$ such that $d = zc \Rightarrow c \big| d$. Therefore any common divisors of the a_i's divides d. Hence, d is the greatest common divisor of a_i, $i = 1, \ldots, n$.

□

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 0.6. (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, $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \Rightarrow \mathfrak{a} \big| \mathfrak{b}$.

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 $\mathfrak{d}\big|\mathfrak{a}$ and $\mathfrak{d}\big|\mathfrak{b}$; if $\mathfrak{c}$ is any ideal such that $\mathfrak{c}\big|\mathfrak{a}$ and $\mathfrak{c}\big|\mathfrak{b}$, then $\mathfrak{c}\big|\mathfrak{d}$.

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), $\mathfrak{a} + \mathfrak{b}\big|\mathfrak{a}$ and $\mathfrak{a} + \mathfrak{b}\big|\mathfrak{b}$. Now suppose there exists an ideal $\mathfrak{c}$ such that $\mathfrak{c}\big|\mathfrak{a}$ and $\mathfrak{c}\big|\mathfrak{b}$. 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 $\mathfrak{c}\big|\mathfrak{a} + \mathfrak{b}$. 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 trivial.

□

Exercise 0.7. (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 $\mathrm{Pic}(\mathfrak{o})$ contains representative ideals prime to a given ideal.

Proof. ??

□