

Commutative Algebra. Theory

Ferran Espuña

December 9, 2023

1 Rings and Ideals

Remark 1.1. Unless otherwise specified, all rings we discuss will be commutative with unit.

Definition 1.2. We say that $I \subseteq A$ is an *ideal* if:

- $(I, +)$ is an abelian group.
- For all $a \in A$ and for all $x \in I$, $ax \in I$.

Definition 1.3. We define:

- The *radical* of an ideal I is $\text{rad}(I) := \{a \in A \mid a^n \in I, n > 0\}$.
- (*Colon ideal*) $(I : J) := \{a \in A \mid aJ \subseteq I\}$.
- (*Saturation*) $(I : J^\infty) := \{a \in A \mid \exists n > 0 \text{ s.t. } aJ^n \subseteq I\}$.

Definition 1.4. Let $f : A \rightarrow B$ be a ring homomorphism, and let $J \subset B$ be an ideal. Then, the *contraction* of J to A is $J^c := \{a \in A \mid f(a) \in J\}$.

Proposition 1.5. In the above situation, J^c is an ideal of A .

Proof. It is an additive subgroup of A as f is an additive group homomorphism. Furthermore, if $a \in J^c$ and $r \in A$, then $f(a) \in J$ so $f(ra) = f(r)f(a) \in J$ as J is an ideal. \square

Definition 1.6. Let R be a ring and $S \subset R$ a subset. Then, the *ideal generated by S* is $\langle S \rangle := \bigcap_{I \supset S} I$, where I ranges over all ideals of R .

Remark 1.7. $\langle S \rangle$ is the smallest ideal of R containing S . It can be checked that it is indeed an ideal by noticing that all elements of it belong to all ideals containing S , and verifying the axioms from there.

Proposition 1.8. *In the above situation,*

$$\langle S \rangle = \{a_1 s_1 + \cdots + a_n s_n \mid n \in \mathbb{N}, a_1, \dots, a_n \in A, s_1, \dots, s_n \in S\}$$

Proof. We will show both inclusions.

(\subset) $\langle S \rangle$ is an ideal containing S , so it contains all elements of the form $a_1 s_1 + \cdots + a_n s_n$.

(\supset) One can easily check that the set on the right is an ideal containing S , so it contains the intersection of all such ideals, which is $\langle S \rangle$.

□

Definition 1.9. Let $f : A \rightarrow B$ be a ring homomorphism, and let $I \subset A$ be an ideal. Then, the *extension* of I to B is $IB = I^e := \langle f(I) \rangle$.

Remark 1.10. I^e is by construction, the smallest ideal of B containing $f(I)$.

Proposition 1.11. *In the above situation, let $I^{ec} := (I^e)^c$, and similarly for the rest. Then:*

1. $I \subset I^{ec}$.
2. $J^{ce} \subset J$
3. $I^e = I^{ece}$
4. $J^c = J^{cec}$

Proof. Note that if K is an ideal of A , then $f(K) \subset K^e$. Furthermore, extension and contraction clearly respect inclusions.

1. $I \subset f^{-1}(f(I)) \subset f^{-1}(I^e) = I^{ec}$.
2. $(J^c)^e = \langle f(J^c) \rangle = \langle f(f^{-1}(J)) \rangle \subset \langle J \rangle = J$.
3. By the two previous points, $(I^e)^{ce} \subset I^e$ and $I \subset I^{ec}$ so $I^e \subset (I^{ec})^e$.
4. Similarly, $J^c \subset (J^c)^{ec}$ and $J^{ce} \subset J$ so $(J^{ce})^c \subset J^c$.

□

Definition 1.12. Let I be an ideal of a ring A . The *quotient ring* A/I is the ring whose elements are the cosets of I in A , and whose operations are defined by

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I \\ (a + I) \cdot (b + I) &= (a \cdot b) + I\end{aligned}$$

Remark 1.13. The sum operation is well defined as it is for all quotient groups. The product operation is well defined as I is an ideal so if $p \in (a + I)$, $q \in (b + I)$, then $pq \in ab + aI + bI + I^2 \subset (ab + I)$.

Proposition 1.14. Let I be an ideal of a ring A . Then, the canonical projection $\pi : A \rightarrow A/I$ is a ring homomorphism.

Proof. It is clearly a group homomorphism. Furthermore, $\pi(a)\pi(b) = (a + I)(b + I) = ab + I = \pi(ab)$. Finally, $\pi(1) = 1 + I$ is clearly the unit of A/I . \square

Definition 1.15. Let $I \subsetneq R$ be an ideal. Then:

- I is *prime* if $ab \in I \Rightarrow a \in I$ or $b \in I$.
- I is *maximal* there are no ideals J such that $I \subsetneq J \subsetneq R$.

We further define the *spectrum* of R as

$$\text{Spec}(R) := \{\mathfrak{p} \subset R \text{ ideal} \mid \mathfrak{p} \text{ is prime}\}.$$

and

$$\text{Max}(R) := \{\mathfrak{m} \subset R \text{ ideal} \mid \mathfrak{m} \text{ is maximal}\}.$$

Proposition 1.16. Let $\mathfrak{p} \subset R$ be an ideal. Then, $\mathfrak{p} \in \text{Spec}(R) \Leftrightarrow R/\mathfrak{p}$ is an integral domain.

Proof. Let

$$\begin{aligned}\pi : R &\rightarrow R/\mathfrak{p} \\ a &\mapsto \bar{a} := a + \mathfrak{p}\end{aligned}$$

be the canonical projection. Then, π is a ring homomorphism. Suppose $a, b \in R$. Then,

$$ab \in \mathfrak{p} \Leftrightarrow \bar{a}\bar{b} = 0$$

$$(a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}) \Leftrightarrow (\bar{a} = 0 \text{ or } \bar{b} = 0)$$

Therefore, as π is surjective, R/\mathfrak{p} is an integral domain if and only if \mathfrak{p} is prime, as both conditions are equivalent to the first condition implying the second. \square

Lemma 1.17. *A ring S is a field if and only if it has no nontrivial ideals $0 \subsetneq I \subsetneq S$*

Proof. We will show both implications.

(\Rightarrow) Let $0 \subsetneq I \subsetneq S$ be an ideal. Then, it has a nonzero element a which must be a unit, so $1 = aa^{-1} \in I$, so $I \subsetneq S = (1) \subset I$, a contradiction.

(\Leftarrow) Let $a \in S$ be nonzero. Then, $(a) \neq 0$ so $(a) = S$, so $1 \in (a)$, so a is a unit. \square

Proposition 1.18. *Let $\mathfrak{m} \subset R$ be an ideal. Then, $\mathfrak{m} \in \text{Max}(R) \Leftrightarrow R/\mathfrak{m}$ is a field.*

Proof. We will use the above characterization of fields. Because the canonical projection $\pi : R \rightarrow R/\mathfrak{m}$ is surjective, Contraction by it respects inequalities, that is $I \subsetneq J \Rightarrow I^c \subsetneq J^c$. On the other hand, for ideals containing \mathfrak{m} , extension by π is just the canonical projection, so $I \subsetneq J \Rightarrow I^e \subsetneq J^e$. Finally, $R^e = R/\mathfrak{m}$ and $(R/\mathfrak{m})^c = R$. Therefore, we have a bijection between nontrivial ideals of R/\mathfrak{m} and ideals $\mathfrak{m} \subsetneq I \subsetneq R$. One of the sets is empty if and only if the other is. \square

Remark 1.19. All fields are integral domains, so $\text{Max}(R) \subset \text{Spec}(R)$. That is, all maximal ideals are prime.

Theorem 1.20. *All rings have maximal ideals.*

Proof. Exercise. Use Zorn's lemma. \square

Theorem 1.21. *Let A be a ring and $I \subseteq A$ be an ideal. Then, there exists a maximal ideal $\mathfrak{m} \subseteq A$ such that $I \subseteq \mathfrak{m}$.*

Proof. Exercise. Use Zorn's lemma. \square

Definition 1.22. We say that a ring R is *local* if it has a unique maximal ideal \mathfrak{m} .

Proposition 1.23. *Let R be a ring. R is local if and only if $R \setminus R^*$ is an ideal (which is then necessarily the maximal ideal).*

Proof. We will show both implications.

(\Rightarrow) Let R be local with maximal ideal \mathfrak{m} . We will show that \mathfrak{m} is exactly $R \setminus R^*$. Let $a \in R \setminus R^*$. Then, $(a) \neq R$ so $(a) \subset \mathfrak{m}$, as it must be contained in some maximal ideal. In particular, $a \in \mathfrak{m}$. On the other hand, if $a \in \mathfrak{m}$, then $(a) \subset \mathfrak{m} \subsetneq R$, so $a \notin R^*$.

(\Leftarrow) Let $I \subsetneq R$ be an ideal. If it contained a unit, then it would contain 1, so $I = R$. Therefore, $I \subset R \setminus R^*$ so the latter is the unique maximal ideal.

□

Definition 1.24. Let R be a ring and $S \subset R$ a subset. We say that S is *multiplicatively closed* if $1 \in S$ and $a, b \in S \Rightarrow ab \in S$.

Definition 1.25. Let R be a ring and $S \subset R$ a multiplicatively closed subset. Then, $S^{-1}R := \{\frac{a}{b} \mid a \in R, b \in S\} / \sim$, where

$$\frac{a}{s} \sim \frac{b}{t} \Leftrightarrow \exists r \in S: r(at - bs) = 0 \quad (1)$$

Proposition 1.26. *In the definition above, \sim is an equivalence relation.*

Proof. The relation is obviously symmetric and reflexive. Let us show that it is transitive. Suppose $\frac{a_1}{s_1} \sim \frac{a_2}{s_2} \sim \frac{a_3}{s_3}$:

$$\begin{aligned} t_1(a_1s_2 - a_2s_1) &= 0 \\ t_2(a_2s_3 - a_3s_2) &= 0 \end{aligned}$$

For some $t_1, t_2 \in S$. Then, multiply the first equation by t_2s_3 and the second by t_1s_1 to get

$$\begin{aligned} t_1t_2s_3a_1s_2 - t_1t_2s_3a_2s_1 &= 0 \\ t_1t_2s_1a_2s_3 - t_1t_2s_1a_3s_2 &= 0 \end{aligned}$$

Adding both equations and collecting like terms, we get

$$0 = t_1 t_2 s_3 a_1 s_2 - t_1 t_2 s_1 a_3 s_2 = t_1 t_2 s_2 (a_1 s_3 - a_3 s_1) \quad (2)$$

Because S is multiplicatively closed, $t_1 t_2 s_2 \in S$, so $\frac{a_1}{s_1} \sim \frac{a_3}{s_3}$. □

Proposition 1.27. *The usual operations*

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \end{aligned}$$

are well defined and make $S^{-1}R$ into a ring.

Proof. Left as an exercise. The arguments are tedious but similar to the above proposition. □

Proposition 1.28. *Let R be a ring and $S \subset R$ a multiplicatively closed subset. Then, the canonical projection*

$$\begin{aligned} \pi : R &\rightarrow S^{-1}R \\ a &\mapsto \frac{a}{1} \end{aligned}$$

is a ring homomorphism. It is injective if and only if S contains no zero divisors.

Proof. $\pi(1) = \frac{1}{1}$ is clearly the unit of $S^{-1}R$. Furthermore, $\pi(a)\pi(b) = \frac{a}{1} \frac{b}{1} = \frac{ab}{1} = \pi(ab)$. $\pi(a) + \pi(b) = \frac{a}{1} + \frac{b}{1} = \frac{1 \cdot a + 1 \cdot b}{1 \cdot 1} = \frac{a+b}{1} = \pi(a+b)$. We have that it is a ring homomorphism. $\text{Ker}(\pi) = \{a \in R \mid \frac{a}{1} \sim \frac{0}{1}\} = \{a \in R \mid \exists s \in S \mid 0 = s(a \cdot 1 + 0 \cdot 1) = sa\}$. Indeed, the kernel is the set of all elements of R that are annihilated by some element of S . In particular, it contains only zero if and only if S contains no zero divisors. □

Proposition 1.29. *Let A be a ring and $S \subset R$ a multiplicatively closed subset. Let $f : A \rightarrow B$ be a ring homomorphism such that $f(S) \subset B^*$. Then, there exists a unique ring homomorphism $g : S^{-1}A \rightarrow B$ such that $f = g \circ \pi$, where π is the canonical projection. That is, the following diagram commutes:*

$$\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\pi \downarrow & \nearrow \exists! g & \\
S^{-1}A & &
\end{array}$$

Proof. Suppose that such a g exists. By definition,

$$g\left(\frac{a}{1}\right) = f(a)$$

For any $s \in S$,

$$1 = f(1) = g\left(\frac{s}{1} \frac{1}{s}\right) = g\left(\frac{s}{1}\right) g\left(\frac{1}{s}\right) \Rightarrow g\left(\frac{1}{s}\right) = g\left(\frac{s}{1}\right)^{-1} = f(s)^{-1}$$

Then,

$$g\left(\frac{a}{s}\right) = g\left(\frac{a}{1} \frac{1}{s}\right) = g\left(\frac{a}{1}\right) g\left(\frac{1}{s}\right) = f(a) f(s)^{-1}$$

Therefore, g is uniquely determined by f . The derived expression for g clearly makes the diagram commute. Finally, we will show that it is well defined and that it is a ring homomorphism. Suppose $\frac{a}{s} = \frac{b}{t}$. Then, for some $u \in S$,

$$u(at - bs) = 0 \Rightarrow 0 = f(0) = f(u(at - bs)) = f(u)(f(a)f(t) - f(b)f(s))$$

But $f(u), f(s), f(t) \in B^*$, so

$$f(a)f(t) = f(b)f(s) \Rightarrow g\left(\frac{a}{s}\right) = f(a)f(s)^{-1} = f(b)f(t)^{-1} = g\left(\frac{b}{t}\right)$$

Therefore, g is well defined. Finally, let us check that it is a ring homomorphism:

- $g\left(\frac{a}{s}\right) + g\left(\frac{b}{t}\right) = f(a)f(s)^{-1} + f(b)f(t)^{-1} = f(a)f(t)f(t)^{-1}f(s)^{-1} + f(b)f(s)f(t)^{-1}f(s)^{-1} = f(at + bs)f(st)^{-1} = g\left(\frac{at+bs}{st}\right) = g\left(\frac{a}{s} + \frac{b}{t}\right)$
- $g\left(\frac{a}{s}\right)g\left(\frac{b}{t}\right) = f(a)f(s)^{-1}f(b)f(t)^{-1} = f(ab)f(st)^{-1} = g\left(\frac{ab}{st}\right) = g\left(\frac{a}{s} \frac{b}{t}\right)$
- $g\left(\frac{1}{1}\right) = 1$

□

Proposition 1.30. *In the above situation, let $I \subset A$ be an ideal. Consider the canonical projection $\pi : A \rightarrow S^{-1}A$. Then we can write the extension of I by π as $I^e =: IS^{-1}A = S^{-1}I := \{\frac{j}{s} \mid j \in I, s \in S\}$. Furthermore, every ideal of $S^{-1}A$ is of this form.*

Proof. It is clear that $S^{-1}I \subset IS^{-1}A$. Suppose that $x = \frac{j_1}{s_1} \frac{a_1}{1} + \dots + \frac{j_n}{s_n} \frac{a_n}{1} \in IS^{-1}A$, with $j_i \in I, a_i \in A, s_i \in S$. Then, by applying the definition of addition repeatedly, we get $x = \frac{j}{s}$, with $j \in I$. Therefore $x \in I^e$.
Now, take any ideal $J \subset S^{-1}A$. We know by 1.11 $J^{ce} \subset J$. We will show the reverse inclusion in this case. Let $\frac{a}{s} \in J$. Then $\pi(a) = \frac{a}{1} = \frac{a}{s} \frac{s}{1} \in J \Rightarrow a \in J^c \Rightarrow \frac{a}{s} \in J^{ce}$. In particular, $J = J^{ce} = J^c S^{-1}A = S^{-1}J^c$. \square

Definition 1.31. (*Total frection ring*) $Tot(A) := S^{-1}A$ where $S = \{a \in A \mid a \text{ is not a zero divisor}\}$.

Definition 1.32. (*Localization at an element*) $A_f := S^{-1}A$ where $S = \{f^n \mid n \geq 0\}$ for a given $f \in A$.

Definition 1.33. Let A be a ring and $\mathfrak{p} \in \text{Spec}(A)$ a prime ideal. Then, the *localization of A at \mathfrak{p}* is $A_{\mathfrak{p}} := S^{-1}A$, where $S = A \setminus \mathfrak{p}$.

Remark 1.34. Indeed, S is multiplicatively closed as \mathfrak{p} is prime.

Proposition 1.35. *In the above situation, $\frac{a}{s} \in A_{\mathfrak{p}}$ is a unit $\iff a \notin \mathfrak{p}$.*

Proof. We will show both implications.

(\Rightarrow) Suppose $\frac{a}{s} \in A_{\mathfrak{p}}$ is a unit. Then, there is some $\frac{b}{t} \in A_{\mathfrak{p}}$ such that $\frac{a}{s} \frac{b}{t} = \frac{1}{1}$. For some $u \notin \mathfrak{p}, u(ab - st) = 0$. Rearranging, $uab = ust$. But neither of u, s, t are in \mathfrak{p} , so their product ust is not in \mathfrak{p} (because \mathfrak{p} is prime). In particular, $a \notin \mathfrak{p}$.

(\Leftarrow) Suppose $a \notin \mathfrak{p}$. Then, $\frac{a}{s} \frac{s}{a} = 1$

\square

Proposition 1.36. *In the above situation, $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.*

Proof. By Proposition 1.23, We just need to show that $\mathfrak{p}A_{\mathfrak{p}} = A_{\mathfrak{p}} \setminus (A_{\mathfrak{p}})^*$. Indeed, by 1.30 we know $\mathfrak{p}A_{\mathfrak{p}} = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}$, which by the previous proposition is exactly the set of nonunits of $A_{\mathfrak{p}}$.

\square