III.D. Ideals

Let R be a commutative domain. We say, given $s, r \in R$, that

(III.D.1) $$s|r \text{ (“}s\text{ divides }r\text{”)} \overset{\text{defn.}}{\iff} r = st \text{ for some } t \in R,$$

and (for $r \notin R^* \cup \{0\}$)

(III.D.2) $$r \text{ is } \textbf{irreducible} \overset{\text{defn.}}{\iff} \begin{pmatrix} r = ab\ (a, b \in R) \\ \implies a \text{ or } b \in R^* \end{pmatrix}.$$

If $u \in R^*$ and $r = su$, one writes $r \sim s$ and says that r and s are **associate**;[9] since $s = ru^{-1}$, this is an equivalence relation. The irreducibles of $\mathbb{Z}$ are clearly the $(\pm)$primes.

Consider $R = \mathbb{Z}[\sqrt{d}]$, equipped with the "norm map"

(III.D.3) $$\begin{aligned} \mathcal{N} \colon R &\to \mathbb{Z} \\ r &\mapsto r\tilde{r}, \end{aligned}$$

where is $r = m + n\sqrt{d}$, $\tilde{r} = m - n\sqrt{d}$.

III.D.4. Lemma. $R^* = \mathcal{N}^{-1}(\{\pm 1\})$.

Proof. Since $\widetilde{rs} = \tilde{r}\tilde{s}$, $\mathcal{N}$ is a homomorphism of multiplicative monoids; and so $\mathcal{N}(R^*) \subset \mathbb{Z}^* = \{\pm 1\}$ ($\implies R^* \subset \mathcal{N}^{-1}(\{\pm 1\})$). If $\mathcal{N}(r) = \pm 1$, then $\tilde{r} = \pm r^{-1} \implies r \in R^*$. $\square$

III.D.5. Proposition. *Let $r \in \mathbb{Z}[\sqrt{d}] \backslash (\mathbb{Z}[\sqrt{d}]^* \cup \{0\})$, and suppose $\mathcal{N}(r) \in \mathbb{Z}$ has no nontrivial ($\neq \pm 1$) proper ($\neq \pm\mathcal{N}(r)$) factors of the form $m^2 - n^2 d$. Then r is irreducible.*

Proof. If $r = ab$, then $\mathcal{N}(r) = \mathcal{N}(a)\mathcal{N}(b)$. By hypothesis, $\mathcal{N}(a)$ or $\mathcal{N}(b) = \pm 1$. Hence a or b is a unit, by III.D.4. $\square$

III.D.6. Example. In $\mathbb{Z}[\sqrt{10}]$,

$$\mathcal{N}(\pm 1 + \sqrt{10}) = -9 \text{ and } \mathcal{N}(3) = 9\,;$$

[9] Alternatively, define r and s to be associate $\iff$ $r|s$ and $s|r$; this is equivalent (why?). If $s|r$ and $r \nmid s$, then s is a **proper factor** of r.

± 3 are not of the form $m^2 - 10n^2$ (HW). Hence, $\pm 1 + \sqrt{10}$ and 3 are irreducible. But

$$(1+\sqrt{10})(-1+\sqrt{10}) = 9 = 3 \cdot 3\,, \tag{III.D.7}$$

and so the analogue of the Fundamental Theorem of Arithmetic I.B.1 *fails*.

This sort of ambiguity was a big problem for attempts to prove Fermat's Last Theorem in the mid-19th Century, or for solving Diophantine equations more generally. A way out was proposed by Kummer, who postulated "ideal elements" into which numbers in the ring augmented by their inclusion would then decompose. For instance, in the case of $\mathbb{Z}[\sqrt{10}]$, these "ideal elements" π_1, π_2 would satisfy[10]

$$\begin{cases} 3 = \pi_1\pi_2 \\ 1+\sqrt{10} = \pi_1^2 \\ -1+\sqrt{10} = \pi_2^2. \end{cases} \tag{III.D.8}$$

Then (III.D.7) becomes $\pi_1^2\pi_2^2 = (\pi_1\pi_2)^2$. Kummer showed that one could construct a theory in which such elements would formally respect divisibility and distributive properties. (Later it was realized that they could be represented by actual elements in the "Hilbert class field of $\mathbb{Q}(\sqrt{10})$".) But Dedekind had the even nicer idea of characterizing an "ideal number" π by its "shadow" in $\mathbb{Z}[\sqrt{10}]$, consisting of *everything (formally) divisible by* π. This is essentially our modern notion of an ideal (in a number ring — the notion in general is due to E. Noether). Indeed, the "shadows" of π_1 and π_2 in the above example will be (in the notation about to be defined) the ideals

$$(3, 1+\sqrt{10}) \quad \text{and} \quad (3, -1+\sqrt{10}). \tag{III.D.9}$$

We will return to this example below.

Turning to some generalities, we have the

[10] To be clear, no actual elements in the ring satisfy these equations.

III.D.10. DEFINITION. A **right** (resp. **left**) **ideal** I in a ring R is an additive subgroup which is closed under right (resp. left) multiplication by all elements of R:

- $\begin{cases} a, b \in I \implies a + b \in I \\ a \in I \implies -a \in I \\ 0 \in I \end{cases}$
- $a \in I,\, r \in R \implies ar \in I$ (resp. $ra \in I$).

An **ideal** $I \subset R$ is a left and right ideal.[11]

Given ideals $I, J \subset R$, $I \cap J$ is clearly an ideal. If $\mathcal{S} \subset R$ is a subset, we define the **ideal generated by** $\mathcal{S}$ by

$$(\mathcal{S}) := \bigcap_{\substack{I \subset R \text{ ideal} \\ I \supset \mathcal{S}}} I. \tag{III.D.11}$$

III.D.12. PROPOSITION. *The ideal $(\mathcal{S})$ consists of all finite sums*

$$r_1 s_1 r_1' + r_2 s_2 r_2' + \cdots + r_k s_k r_k'$$

where $r_i, r_i' \in R$, $s_i \in \mathcal{S}$, and $k \in \mathbb{N}$.

PROOF. By the closure properties of III.D.10, all such finite sums must belong to $(\mathcal{S})$. By associativity and distributivity, the set of such sums is itself closed under addition and multiplication by R, hence is one of the ideals being intersected in RHS(III.D.11), and as such contains $(\mathcal{S})$. $\square$

III.D.13. DEFINITION. Given $I \subset R$ an ideal, I is

- **finitely generated** $\iff I = (\mathcal{S})$ for some finite subset $\mathcal{S} \subset R$.
- **principal** $\iff I = (a)$ for some element $a \in R$.

Note that if R is commutative, then $(a) = \{ra \mid r \in R\}$, and

$$(a_1, \ldots, a_m) = \{r_1 a_1 + \cdots r_m a_m \mid r_1, \ldots, r_m \in R\}.$$

[11]Note that this is a stronger notion than being a "subrng" because of the closure under multiplication by *elements of* R. And yes, I mean "subrng" not "subring": except for R itself, ideals in R do not contain 1.

We can also consider "sums" and "products" of ideals: define

$$\text{(III.D.14)} \qquad \begin{cases} I+J := (I \cup J) = \{a+b \mid a \in I,\ b \in J\} \\ IJ := (I \odot J) = \{\sum_{i=1}^{k} a_i b_i \mid a_i \in I,\ b_i \in J,\ k \in \mathbb{N}\}, \end{cases}$$

where $I \odot J$ is the set of products $\{ab \mid a \in I, b \in J\}$. To state the obvious:

III.D.15. PROPOSITION. *Suppose* $I = (\mathcal{S})$ *and* $J = (\mathcal{T})$.
(i) $I + J = (\mathcal{S} \cup \mathcal{T})$.
(ii) *If* R *is commutative, then* $IJ = (\{st \mid s \in \mathcal{S},\ t \in \mathcal{T}\}) = (\mathcal{S} \odot \mathcal{T})$.
(iii) *In particular, if* $I = (a)$ *and* $J = (b)$, *then* $I + J = (a, b)$ *and (for* R *commutative)* $IJ = (ab)$.

Furthermore, if R is commutative and $a, b \in R$, we have

III.D.16. PROPOSITION ("Caesar's lemma"). *To divide is to contain:*[12]

$$a|b \iff (a) \supseteq (b).$$

PROOF. If $ra = b$, then

$$(b) = (ra) = \{r'ra \mid r' \in R\} \subset \{r''a \mid r'' \in R\} = (a).$$

Conversely, $(a) \supset (b) \implies b \in (a) \implies b = ra$ for some $r \in R$. $\square$

III.D.17. EXAMPLE. Returning to III.D.6 *ff* and $R = \mathbb{Z}[\sqrt{10}]$, we compute

$$\begin{aligned}(3, 1+\sqrt{10})^2 &= \left(9,\ 3+3\sqrt{10},\ 11+2\sqrt{10}\right) \\ &= \left((1+\sqrt{10})(-1+\sqrt{10}),\ (1+\sqrt{10})3,\ (1+\sqrt{10})(1+\sqrt{10})\right) \\ &\subset (1+\sqrt{10}),\end{aligned}$$

[12] A rough translation into algebra-ese of J. Caesar's famous maxim "divide et impera". I jest, but this is useful as a mnemonic device for remembering the rule.

making use of III.D.15(ii) to square the ideal.[13] Similarly one shows that $(3,-1+\sqrt{10})^2 \subset (-1+\sqrt{10})$ and

$$\begin{aligned}(3,1+\sqrt{10})(3,-1+\sqrt{10}) &= \left(9,\, 3+3\sqrt{10}\, -3+3\sqrt{10}\right) \\ &\subset (3).\end{aligned}$$

For the reverse inclusions,[14]

$$\begin{aligned}1+\sqrt{10} = -(11+2\sqrt{10}) + 9 + (3+3\sqrt{10}) \;\in (3,1+\sqrt{10})^2 \\ \implies \quad (1+\sqrt{10}) \subset (3,1+\sqrt{10})^2,\end{aligned}$$

and similarly $(-1+\sqrt{10}) \subset (3,-1+\sqrt{10})^2$; while

$$\begin{aligned}&3 = 9-(3+3\sqrt{10}) + (-3+3\sqrt{10}) \;\in\; (3,1+\sqrt{10})(3,-1+\sqrt{10}) \\ &\implies (3) \subset (3,1+\sqrt{10})(3,-1+\sqrt{10}).\end{aligned}$$

So if we set $I_1 = (3,1+\sqrt{10})$ and $I_2 = (3,-1+\sqrt{10})$, we indeed have

$$I_1 I_2 = (3)\,, \;\; I_1^2 = (1+\sqrt{10})\,, \;\; \text{and } I_2^2 = (-1+\sqrt{10})$$

and the ideals serve their intended function, recovering an analogue of (III.D.8).

Returning to the setting of a general ring R, let $I \subsetneq R$ be a *proper* ideal. Clearly, this is a normal subgroup of the additive (abelian) group, and so we can construct the (additive) quotient group R/I. Its elements are the equivalence classes defined by the equivalence relation

$$a \equiv b \quad \Longleftrightarrow \quad a-b \in I.$$

That is, they are the cosets $a+I$, with the addition rule

$$(a+I)+(b+I) = (a+b)+I. \tag{III.D.18}$$

[13] This is an important point: the product $(a,b)(c,d)$ is the ideal generated by the set of products $\{a,b\} \odot \{c,d\} := \{ac, ad, bc, bd\}$.

[14] The basic principle being applied here (in the case of 1-element sets) is that if a set $\mathcal{S}$ is contained in an ideal I, then $(\mathcal{S}) \subset I$.

We now define a multiplicative structure on R/I by the rule

$$(a+I)(b+I) := ab + I, \tag{III.D.19}$$

with identity coset $1+I$. The main check required is that (III.D.19) is well-defined: given $a' = a+\alpha \in a+I$ and $b' = b+\beta \in b+I$,

$$\begin{aligned}(a'+I)(b'+I) = a'b' + I &= (a+\alpha)(b+\beta) + I \\ &= ab + \underbrace{\alpha b + a\beta + \alpha\beta}_{\in I} + I \\ &= ab + I.\end{aligned}$$

Distributivity is clear from (III.D.18)-(III.D.19) and distributivity in R. Hence, R/I has the structure of a ring.

III.D.20. REMARK. In our study of groups, we had two "stupid quotients", $G/\langle 1\rangle (\cong G)$ and $G/G (\cong \{1\})$. Here, the only stupid quotient ring is $R/(0) = R$; because $\{0\}$ is not a ring, we cannot consider R/R, and accordingly the definition of quotient ring requires a *proper* ideal.

III.D.21. EXAMPLES. (i) $(n) = n\mathbb{Z} \subset \mathbb{Z}$ is a proper ideal ($n > 1$), and $\mathbb{Z}/(n)$ (or $\mathbb{Z}/n\mathbb{Z}$) is just $\mathbb{Z}_n$ (viewed as a ring).

(ii) In $\mathbb{Z}[x]/(x^2-10)$, any element is of the form $P(x) + (x^2-10)$ (where (x^2-10) is the principal ideal). Applying polynomial division, this equals $\{x^2-10\}\cdot Q(x) + R(x) + (x^2-10) = R(x) + (x^2 - 10)$, where $R(x) = ax+b$.

(iii) In the ring $C^0(\mathcal{M})$ of continuous functions on a manifold $\mathcal{M}$, the subset $I_{\mathcal{S}}$ of functions identically zero on a subset $\mathcal{S} \subset \mathcal{M}$ is an ideal. In $C^0(\mathcal{M})/I_{\mathcal{S}}$, cosets $f + I_{\mathcal{S}}$ and $g + I_{\mathcal{S}}$ are the same $\iff f - g \in I_{\mathcal{S}}$ $\iff$ f and g have the same restriction to $\mathcal{S}$. So the quotient can be thought of as a ring of functions on $\mathcal{S}$ of some sort.

(iv) We can consider $\mathbb{Z}[\sqrt{10}]$ modulo the ideals (3), $(\pm 1 + \sqrt{10})$, and $(3, \pm 1 + \sqrt{10})$.

(v) Let R be commutative. While there are *left* [resp. *right*] *ideals* in $M_n(R)$ (e.g. matrices with last column [resp. row] zero) that "take advantage of the matrix structure", there are no (2-sided) *ideals* that do this:

III.D.22. PROPOSITION. *If $I \subset R$ is an ideal, then $M_n(I) \subset M_n(R)$ is an ideal.*[15] *In fact, all ideals of $M_n(R)$ arise in this way.*

PROOF. If $A \in M_n(I)$, $B \in M_n(R)$, then entries $\sum_k a_{ik}b_{kj}$ of AB are obviously in I, hence $AB \in M_n(I)$.

Let $J \subset M_n(R)$ be an ideal, and let

$$I := \{a \in R \mid a \text{ is an entry in some matrix belonging to } J\}.$$

Then $J \subset M_n(I)$.

To show I is an ideal: given $A \in J$, J contains

$$\mathbf{e}_{ki}A\mathbf{e}_{j\ell} = \mathbf{e}_{ki}(\textstyle\sum_{m,n} a_{mn}\mathbf{e}_{mn})\mathbf{e}_{j\ell} = \textstyle\sum_{m,n} a_{mn}\delta_{im}\delta_{nj}\mathbf{e}_{k\ell} = a_{ij}e_{k\ell}.$$

Hence for all $a \in I$ for all k, ℓ, we have $a\mathbf{e}_{k\ell} \in J$. Now for $\alpha, \beta \in I$, $r \in R$,

$$\alpha\mathbf{e}_{11}, \beta\mathbf{e}_{11} \in J \implies \begin{cases} (\alpha+\beta)\mathbf{e}_{11} = \alpha\mathbf{e}_{11} + \beta\mathbf{e}_{11} \in J \implies \alpha+\beta \in I \\ \alpha r\mathbf{e}_{11} = \alpha\mathbf{e}_{11} \cdot r\mathbf{e}_{11} \in J \implies \alpha r \in I \end{cases}$$

(and similarly for $r\alpha$, $-\alpha$).

To show $J \supset M_n(I)$: given elements $\alpha_{ij} \in I$, each $\alpha_{ij}\mathbf{e}_{ij} \in J$ (by the last paragraph). Thus, a general element $\sum_{i,j} \alpha_{ij}\mathbf{e}_{ij}$ of $M_n(I)$ belongs to J. $\square$

What about ideals in $\mathbb{Q}$, $\mathbb{Q}[\mathbf{i}]$, $\mathbb{R}$, $\mathbb{C}$?

III.D.23. THEOREM. *Let R be a commutative ring. Then*

$$R \text{ is a field} \iff R \text{ has no nontrivial proper ideals.}$$

PROOF. ($\implies$): Let $I \subset R$ be a nontrivial ideal, $a \in I\backslash\{0\}$. Given any $b \in R$, $b = a(a^{-1}b) \in I$, so $I = R$.

($\impliedby$): Let $a \in R\backslash\{0\}$; then $(a) = \{ar \mid r \in R\}$ contains $\{a\}$ hence is nontrivial. By hypothesis, it must be R. Hence for any $b \in R$, there is an $r \in R$ such that $ar = b$; take $b = 1$. $\square$

[15] e.g., $M_n(p\mathbb{Z}) \subset M_n(\mathbb{Z})$

Notice where the proof of "($\Longleftarrow$)" breaks down for something like $R = M_n(\mathbb{C})$ (which satisfies the hypothesis on ideals by III.D.22): we get that $\{\sum_i r_i a r_i' \mid r_i, r_i' \in R\} = R$, which *doesn't* imply that a is invertible.

At this point, we should mention the key example:

III.D.24. PROPOSITION. *$\mathbb{Z}_m$ is a field $\iff$ m is prime.*

PROOF. ($\Longrightarrow$): obvious, since m composite $\Longrightarrow$ $\mathbb{Z}_m$ not a domain.

($\Longleftarrow$): Given $a + (m)$ (or "$\bar{a}$") in $\mathbb{Z}_m \backslash \{0\}$, with $a \in \{1, \ldots, m - 1\}$, we know that the gcd of m and a is 1 (as m is prime). So there exist $k, \ell \in \mathbb{Z}$ such that $ka + \ell m = 1 \implies (k + (m))(a + (m) = 1 - \ell m + (m) = 1 + (m)$. $\square$

Before turning to homomorphisms, here is one more

III.D.25. DEFINITION. An **ascending chain** of ideals is a nested sequence

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq R$$

of ideals. Note that this is a chain in the set-theoretic sense (totally ordered), while the set of all ideals is partially ordered by inclusion.

III.D.26. LEMMA. *The union $\cup_{j \geq 1} I_j \subset R$ is an ideal. More generally, for any chain $\mathcal{C}$ in the set of ideals of R, $\cup_{J \in \mathcal{C}} J$ is an ideal of R.*

PROOF. Any element (or pair of elements) of the union is contained in some member $J_0 \in \mathcal{C}$, because of the total ordering. By the closure properties III.D.10 of J_0, the sum of these elements and their products by elements of R are contained in J_0 hence in $\cup_{J \in \mathcal{C}} J$. So this union satisfies the closure properties too. $\square$

III.D.27. THEOREM. *Let $I \subsetneq R$ be a proper ideal. Then there exists a maximal proper ideal I_0 which contains I.* (*Here "maximal" means merely that there is no ideal J with $I_0 \subsetneq J \subsetneq R$.*)

PROOF. Let $\mathcal{P}$ denote the set of *proper* ideals of R containing I, partially ordered by $\subseteq$, and let $\mathcal{C}$ be a chain in $\mathcal{P}$. Consider the set

$\mathcal{I}_{\mathcal{C}} := \cup_{J\in\mathcal{C}} J$, which by the Lemma is an ideal. Clearly, since every J contains I and doesn't contain 1, $\mathcal{I}_{\mathcal{C}} \supset I$ and $1 \notin \mathcal{I}_{\mathcal{C}}$, which implies $\mathcal{I}_{\mathcal{C}} \in \mathcal{P}$.

We have shown that every chain in $\mathcal{P}$ has an upper bound (in $\mathcal{P}$). So Zorn produces a maximal element in $\mathcal{P}$, which must be a maximal proper ideal containing I. $\square$