III. Rings

III.A. Examples of rings

The theory of rings and ideals grew out of several 19th and early 20th Century sources:

• polynomials (Gauss, Eisenstein, Hilbert, etc.);
• number rings (Dirichlet, Kummer [“ideal numbers”], Kronecker, Dedekind [“ideals in number rings”], Hilbert, etc.); and
• matrix rings and hypercomplex numbers (Hamilton [quaternions], Cayley [octonions], etc.).

Specifically, the term \( \text{Zahlring} \) showed up in the study of what we would now call rings of integers in algebraic number fields; e.g. cyclotomic rings such as \( \mathbb{Z}[\zeta_5] \) (\( \zeta_5 = \text{a 5th root of 1} \)) arose in the context of attempts to prove Fermat’s last theorem, and \( \zeta_5 \) “cycles back to itself” (suggesting a ring) upon repeatedly taking powers. Here is the modern definition, due to E. Noether (\(~1920\)):

III.A.1. Definition. A ring \((R, +, \cdot, 0, 1)\) comprises a set \(R\) together with 2 binary operations and distinguished elements, satisfying:

(i) \((R, +, 0)\) is an abelian group;
(ii) \((R, \cdot, 1)\) is a monoid; and
(iii) distributive laws:

\[ r(s_1 + s_2) = rs_1 + rs_2 \quad \text{and} \quad (r_1 + r_2)s = r_1s + r_2s. \]

Note that we do not assume the existence of multiplicative inverses.

III.A.2. Remark. (i) If we didn’t assume that “+” was commutative, this would be forced upon us by the distributive laws as follows:
• \(-(a + b) = (-b) + (-a)\) (not assuming \((R, +, 0)\) abelian)

• \(\exists\) “additive” inverse \(-1\) of 1 (since \((R, +, 0)\) is a group)

• adding \(-0r\) on the left to \(0r = (0 + 0)r = 0r + 0r\) gives \(0 = 0r\)

• adding \((-r)\) on the right to \((-r) + r = 0 = (1 - 1)r = (-1)r + 1r = (-1)r + r\) gives \(-r = (-1)r\)

• \(- (a + b) = (-1)(a + b) = (-1)a + (-1)b = (-a) + (-b)\).

(ii) There is also the notion of a “rng” \((R, +, \cdot, 0)\) where \((R, \cdot)\) is taken to be a “semigroup”, meaning that one doesn’t assume the existence of a multiplicative “identity” (or inverses). However, we can construct a ring containing \(R\) with underlying set \(S = \mathbb{Z} \times R\), operations

\[
\begin{align*}
(n_1, r_1) + (n_2, r_2) &:= (n_1 + n_2, r_1 + r_2) \quad \text{and} \\
(n_1, r_1) \cdot (n_2, r_2) &:= (n_1n_2, n_1r_2 + n_2r_1 + r_1r_2),
\end{align*}
\]

and distinguished elements \(1 := (1, 0)\) and \(0 := (0, 0)\), by checking that the associative and distributive laws hold. (\(R\) consists of the elements \((0, r)\).)

(iii) A **subring** of \(R\) is a subset closed under \(+, -\), and \(\cdot\). Hence the intersection of subrings is a subring, and it makes sense to speak of the subring generated by a subset \(S\) (= intersection of all subrings containing \(S\)).

(iv) A ring is called **commutative** if the multiplication “\(\cdot\)” is. (We don’t use the term “abelian” for rings.)

III.A.3. **Examples.** (i) \((\mathbb{A}, +, \cdot, 0, 1)\), with \(\mathbb{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\), or \(\mathbb{Z}_m\).

(ii) Direct \(\prod_{i \in I} R_i \oplus_{i \in I} R_i\). If \(|I| < \infty\) then these are the same. Otherwise, the \(\prod_{i \in I} R_i\) consists of \(\infty\)-tuples

\[
\begin{align*}
\{ &\text{products of rings} \} &\text{with no constraints} \\
\{ &\text{sums of rings} \} &\text{with all but finitely many entries zero.}
\end{align*}
\]

\[\text{1The products are also written } \times_{i \in I} R_i, \text{ more typically when there are finitely many, viz. } R_1 \times \cdots \times R_k. \text{ We won’t use “} \oplus \text{” for finite sums/products of rings.} \]
(iii) **Number rings.** Let $D$ be a squarefree integer, i.e. $\pm p_1 \cdots p_d$ where $p_1, \ldots, p_d$ are distinct primes. Inside $\mathbb{C}$ (or $\mathbb{R}$, if $D > 0$), it is easy to see the closure properties for the **(quadratic) number field**

$$Q[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

and the **(quadratic) number ring**

$$\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}.$$ 

What about

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}] := \{m + n\left(\frac{1+\sqrt{D}}{2}\right) \mid m, n \in \mathbb{Z}\}$$

$$= \left\{\frac{a+b\sqrt{D}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \right\}?$$

(For the last equality, take $m = \frac{a-b}{2}$ and $n = b$.) Of course, the issue is multiplicative closure:

$$(m + n\left(\frac{1+\sqrt{D}}{2}\right))(m' + n'\left(\frac{1+\sqrt{D}}{2}\right)) =$$

$$mm' + (mn' + nm')(\frac{1+\sqrt{D}}{2}) + \frac{mn'(1+D) + 2\sqrt{D}}{4}.$$ 

Clearly closure holds $\iff 4 \mid D - 1 \iff D \equiv 1 \pmod{4}$. As we shall see, the “ring of integers” in $Q[\sqrt{D}]$ is

$$\begin{cases} 
\mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 \pmod{4} \\
\mathbb{Z}[\sqrt{D}] & \text{otherwise.}
\end{cases}$$

Two special cases of interest are $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and $\mathbb{Z}[i]$.

(iv) **Polynomial rings.** Let $R$ be a commutative ring. Set

$$R[x] := \{\text{sequences } (r_0, r_1, \ldots, r_n, 0, 0, \ldots) \mid r_i \in R\}$$

zero from some point on.
and define, given \( \mathbf{a} = (a_k)_{k \geq 0} \) and \( \mathbf{b} = (b_k)_{k \geq 0} \),
\[
\mathbf{a} + \mathbf{b} := (a_k + b_k)_{k \geq 0} \quad \text{and} \quad \mathbf{a} \cdot \mathbf{b} := (\sum_{j=0}^{k} a_j b_{k-j})_{k \geq 0}.
\]
Also put \( \mathbf{0} := (0, 0, 0, \ldots) \) and \( \mathbf{1} := (1, 0, 0, \ldots) \). Then we have
\[
(\mathbf{a} + \mathbf{b}) \cdot \mathbf{c} = (\sum_{j=0}^{k} (a_j + b_j) c_{k-j})
= (\sum_{j=0}^{k} a_j c_{k-j}) + (\sum_{j=0}^{k} b_j c_{k-j}) = \mathbf{a} \cdot \mathbf{c} + \mathbf{b} \cdot \mathbf{c}
\]
and
\[
(\mathbf{a} \cdot \mathbf{b}) \cdot \mathbf{c} = (\sum_{i=0}^{k} a_i b_{k-i}) \cdot \mathbf{c} = (\sum_{\ell=0}^{k} (\sum_{i=0}^{\ell} a_i b_{\ell-i}) c_{\ell-i})
= (\sum_{i=0}^{k} \sum_{j=0}^{i} b_j c_{(k-i)-j}) = \mathbf{a} \cdot (\sum_{j=0}^{k} b_j c_{k-j})
= \mathbf{a} \cdot (\mathbf{b} \cdot \mathbf{c}),
\]
so that II.A.1(iii) is satisfied.

Now identify \( \mathbb{R} \) with the subring \( \{(r, 0, 0, \ldots) \} \subset \mathbb{R}[x] \). Taking \( x := (0, 1, 0, 0, \ldots) \), we have \( x^n = (0, \ldots, 0, 1, 0, 0, \ldots) \) so that
\[
(r_0, r_1, r_2, \ldots, r_n, 0, 0, \ldots) = r_n x^n + \cdots + r_1 x + r_0,
\]
which is obviously a much more appealing (and standard) notation. We can also (inductively) define polynomial rings in several variables by
\[
\mathbb{R}[x_1, \ldots, x_n] := (\mathbb{R}[x_1, \ldots, x_{n-1}])[x_n].
\]
For any \( r \in \mathbb{R} \), we can consider the evaluation map
\[
\text{ev}_r : \mathbb{R}[x] \longrightarrow \mathbb{R}
\]
sending \( r_n x^n + \cdots + r_1 x + r_0 \longmapsto r_n r^n + \cdots + r_1 r + r_0. \)
More generally, we can take the product
\[
\prod_{r \in \mathbb{R}} \text{ev}_r : \mathbb{R}[x] \rightarrow \prod_{\mathbb{R}} \mathbb{R} (= \mathbb{R}^{\mathbb{R}})
\]
of all such maps, sending a polynomial to (essentially) its “graph”. This is not always surjective (e.g. if \( \mathbb{R} = \mathbb{R} \)) or injective (e.g. if \( \mathbb{R} = \mathbb{Z}_3 \)).
(v) **Quaternions.** The ring version is built out of the group one: put

\[ \mathbb{H} := \{ a + i + cj + dk \mid a, b, c, d \in \mathbb{R} \}, \]

where \( i, j, k \) have the same multiplicative properties as in the 8-element group \( \mathbb{Q} \). Clearly this is noncommutative. The "H", of course, is for Hamilton.

(vi) **Matrix rings.** Let \( R \) be an arbitrary ring, \( n \in \mathbb{N} \). We define a ring with underlying set

\[ M_n(R) := \{ \sum_{i,j=1}^n r_{ij} e_{ij} \mid r_{ij} \in R \}, \]

where the \( e_{ij} \) are formal symbols. Taking \( A = \sum_{i,j} a_{ij} e_{ij}, B = \sum_{i,j} b_{ij} e_{ij}, \) we set

\[ 0 := \sum_{i,j=1}^n 0 e_{ij}, 1 := \sum_{i,j=1}^n \delta_{ij} e_{ij} = \sum_{i=1}^n e_{ii}, \]

and

\[ A + B := \sum_{i,j=1}^n (a_{ij} + b_{ij}) e_{ij} \quad \text{and} \quad AB := \sum_{i,j=1}^n (\sum_{k=1}^n a_{ik} b_{kj}) e_{ij}. \]

Associativity follows from

\[ (AB)C = \sum_{i,j=1}^n (\sum_{k=1}^n a_{ik} c_{kj}) e_{ij} = A(BC) \]

and the associativity of \( R \); the rest is left to you.\(^3\) Of course, these can be represented in the standard way as matrices

\[ A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \]

and you may think of \( e_{ij} \) as the matrix with a 1 at the \((i,j)\)th place and zeroes elsewhere. We have

\[ e_{ij} e_{k\ell} = \begin{cases} 0, & j \neq k \\ e_{i\ell}, & j = k. \end{cases} \]

The noncommutativity is highly visible this way.

\(^2\)Here \( \delta_{ij} (= 1 \text{ if } i = j, \text{ and } 0 \text{ otherwise}) \) is the Kronecker delta.

\(^3\)It is important to realize here that the order matters, not just of \( AB \) vs. \( BA \), but of \( a_{ik} b_{kj} \) vs. \( b_{kj} a_{ik} \), because \( R \) may not be commutative.
Here are some definitions which were clearly not possible (or not interesting) for groups.

III.A.4. Definition. Let $R$ be a ring, $r \in R$ an element.
(i) $r$ is a left [resp. right] zero-divisor $\iff \exists r' \in R \setminus \{0\}$ such that $rr' = 0$ [resp. $r'r = 0$].
(ii) $r$ is nilpotent $\iff \exists n \in \mathbb{N}$ such that $r^n = 0$.
(iii) $r$ is idempotent $\iff r^2 = r$.

These are easily illustrated in $M_2(\mathbb{R})$:

III.A.5. Example. (i) In $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$, the boxed element is a left zero-divisor.
(ii) In $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0$, the boxed element is nilpotent.
(iii) In $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, the boxed element is idempotent. (Think projection.)

III.A.6. Definition. The characteristic of a ring $R$ is the (smallest) number of times one has to add 1 (the multiplicative identity element of $R$) to itself to obtain 0, unless this is not possible. In the latter case, the characteristic is zero.

III.A.7. Examples. (i) $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, M_2(\mathbb{R}), \mathbb{Q}[x]$ all have char$(R) = 0$.
(ii) $R = \mathbb{Z}_m, M_n(\mathbb{Z}_m), \mathbb{Z}_m[x]$ have char$(R) = m$.
(iii) In a general commutative ring, we have

\[
(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.
\]

If char$(R) = p$, then $p | \binom{p}{k}$ for $0 < k < p \implies$

\[
(x + y)^p = x^p + y^p,
\]

the so-called “Freshman’s dream”.

Next are some definitions analogous to those in groups or monoids:

III.A.10. Definition. The center of $R$ is

\[
C(R) := \{ r \in R \mid rs = sr \forall s \in R \}.
\]
III.A.11. EXAMPLES. (i) $C(\mathbb{H}) = \mathbb{R}$.

(ii) If $R$ is commutative, $C(M_n(R)) = R$, where $R$ is identified with the subring of diagonal matrices $\begin{pmatrix} r & 0 \\ 0 & \ddots & \ddots \\ \vdots & \ddots & \ddots \\ 0 & \ddots & \ddots & r \end{pmatrix} = r1 = "r"$. More generally, $C(M_n(R)) = C(R)$.

PROOF. Given $A \in C(M_n(R))$,

$$0 = Ae_{k\ell} - e_{k\ell}A = \sum_{i,j=1}^{n} a_{ij}(e_{ij}e_{k\ell} - e_{k\ell}e_{ij})$$

$$= \sum_{i=1}^{n} a_{ik}e_{i\ell} - \sum_{j=1}^{n} a_{\ell j}e_{kj}.$$ 

In particular, the $(k, \ell)^{th}$ entry of the last line is $a_{kk} - a_{\ell\ell}$ and the $(i, \ell)^{th}$ entry (for $i \neq k$) is $a_{ik}$. So off-diagonal entries of $A$ are 0 and the diagonal ones are all equal. Finally, consider $Ar - rA$. \qed

III.A.12. DEFINITION. $r \in R$ is a unit (or invertible) $\iff \exists r' \in R$ such that $rr' = 1 = r'r$. (It is not enough in a general noncommutative ring to have $rr' = 1$ or $r'r = 1$ for invertibility.) The units in $R$ form a group $R^*$ under multiplication.\footnote{In Jacobson, $R^*$ means $R \setminus \{0\}$, and $U(R)$ is the group of units. We will not use this notation; the notation given above is more standard.}

To begin with a few easy examples: for $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$, and more generally for division rings (see the next section), the units $R^*$ are all nonzero elements. But that is not its general meaning. For instance, we have $\mathbb{Z}^* = \{\pm 1\}$ and $\mathbb{Z}_8^* = \{1, 3, 5, 7\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Another example is $M_n(\mathbb{R})^* = \text{GL}_n(\mathbb{R})$, which everyone knows is the matrices with determinant in $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. But for matrices over a more general ring $R$? You’d think determinants might help, but not if $R$ is noncommutative:

III.A.13. EXAMPLE. Consider $\begin{pmatrix} k & 1 \\ j & 1 \end{pmatrix} \in M_2(\mathbb{H})$. The "determinant" $ki - 1j = j - j = 0$, but

$$\begin{pmatrix} k & 1 \\ j & 1 \end{pmatrix} \begin{pmatrix} \frac{-1}{2} & \frac{-1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$
So we can only hope for invertibility of matrices to be easily detected via determinants when the entries are in a commutative ring.

Another key example of units in a commutative ring is problem #7 from HW 1. Recall that this produced a group structure \( \cong \mathbb{Z} \times \mathbb{Z}_2 \) on integer solutions to \( x^2 - 5y^2 = \pm 4 \). I claim that this can be interpreted as an isomorphism

\[
\mathbb{Z} \times \mathbb{Z}_2 \cong \left( \mathbb{Z} \left[ \frac{1 + \sqrt{5}}{2} \right] \right)^* \quad (a, \pm 1) \mapsto \pm \left( \frac{1 + \sqrt{5}}{2} \right)^a.
\]

Given \( \alpha = \frac{x + y\sqrt{5}}{2} \in R := \mathbb{Z} \left[ \frac{1 + \sqrt{5}}{2} \right] \), write \( \tilde{\alpha} := \frac{x - y\sqrt{5}}{2} \in R \). The composition law that led to the group structure on LHS(III.A.14) was exactly multiplication in \( R \). Moreover, \((x, y)\) solves the above equation \( \iff \alpha \cdot (\pm \tilde{\alpha}) = 1 \implies \alpha \in R^* \). Conversely, if \( \alpha \in R^* \), then there exists \( \alpha' = \frac{x' + y'\sqrt{5}}{2} \in R \) with \( \alpha \alpha' = 1 \), and then \( (\alpha \tilde{\alpha}) (\alpha' \tilde{\alpha}') = \alpha \alpha' \tilde{\alpha} \tilde{\alpha}' = 1 \). Since \( x \equiv y \pmod{2} \), we have that \( x^2 \equiv 5y^2 \pmod{4} \implies \alpha \tilde{\alpha} = \frac{x^2 - 5y^2}{4} \in \mathbb{Z} \), and similarly for \( \alpha' \tilde{\alpha}' \). So the only way the product of \( \alpha \tilde{\alpha} \) and \( \alpha' \tilde{\alpha}' \) is 1, is if they are both \( \pm 1 \), and then \( \alpha \in R^* \).

So far we have discussed only quadratic number fields and number rings. To give a brief glimpse ahead, a general result of Dirichlet says that for a number field \( K \) with \( r_1 \) distinct real embeddings and \( r_2 \) pairs of conjugate complex embeddings,

\[
O_K^* \cong \mathbb{Z}^{r_1 + r_2 - 1} \times \{ \text{torsion group} \},
\]

where \( O_K \subset K \) is the ring of integers of \( K \). The main point is that (III.A.14) is a special case (with \( r_1 = 2 \) and \( r_2 = 0 \)) of a much more general result.

\[\text{All number fields can be viewed as vector spaces over } \mathbb{Q} \text{ of some finite dimension, called the degree } [K: \mathbb{Q}]. \text{ In this case, that degree is } r_1 + 2r_2. (\text{An embedding of fields means an injective homomorphism, in this case into } \mathbb{R} \text{ or } \mathbb{C}. \text{ These notions will be discussed later.) The case } K = \mathbb{Q}[\sqrt{D}] \text{ has } r_1 = 0 \text{ and } r_2 = 1 \text{ if } D < 0, \text{ or } r_1 = 2 \text{ and } r_2 = 1 \text{ if } D > 0.\]