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 *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 $\mathbb{Z}[\zeta_5]$ ($\zeta_5 =$ a 5th root of 1) arose in the context od attempts to prove Fermat's last theorem, and ζ_5 "cycles back to itself" (suggesting a ring) upon repeatedly taking powers. Here is the modern definition, due to E. Noether ($\sim$1920):

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

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

$$r(s_1 + s_2) = rs_1 + rs_2 \quad \text{and} \quad (r_1 + r_2)s = r_1 s + r_2 s.$$

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 $(-r) + r = 0 = 0r = (-1+1)r = (-1)r + 1r = (-1)r + r$ gives $-r = (-1)r$
- $-(a+b) = (-1)(a+b) = (-1)a + (-1)b = (-a) + (-b)$.

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

$$\begin{cases} (n_1, r_1) + (n_2, r_2) := (n_1 + n_2, r_1 + r_2) & \text{and} \\ (n_1, r_1) \cdot (n_2, r_2) := (n_1 n_2, n_1 r_2 + n_2 r_1 + r_1 r_2), \end{cases}$$

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 $\bullet$. Hence the intersection of subrings is a subring, and it makes sense to speak of the subring generated by a subset $\mathcal{S}$ (= intersection of all subrings containing $\mathcal{S}$).

(iv) A ring is called **commutative** if the multiplication "$\bullet$" is. (We don't use the term "abelian" for rings.)

III.A.3. EXAMPLES. (i) $(\mathbb{A}, +, \bullet, 0, 1)$, with $\mathbb{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_m$.

(ii) Direct $\begin{cases} \text{products} \\ \text{sums} \end{cases}$ of rings[1] $\begin{cases} \prod_{i \in I} R_i \\ \oplus_{i \in I} R_i \end{cases}$. If $|I| < \infty$ then these are the same. Otherwise, the $\begin{cases} \prod \\ \oplus \end{cases}$ consists of ∞-tuples

$$\begin{cases} \text{with no constraints} \\ \text{with all but finitely many entries zero.} \end{cases}$$

[1] The products are also written $\times_{i \in I} R_i$, more typically when there are finitely many, viz. $R_1 \times \cdots \times R_k$. We won't use "$\oplus$" 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**

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

and the **(quadratic) number ring**

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

What about

$$\begin{aligned} \mathbb{Z}[\tfrac{1+\sqrt{D}}{2}] :&= \{m + n(\tfrac{1+\sqrt{D}}{2}) \mid m, n \in \mathbb{Z}\} \\ &= \{\tfrac{a+b\sqrt{D}}{2} \mid a, b \in \mathbb{Z},\ a \underset{(2)}{\equiv} b\}\,? \end{aligned}$$

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

$$\begin{aligned} (m + n(\tfrac{1+\sqrt{D}}{2}))(m' + n'(\tfrac{1+\sqrt{D}}{2})) \ &= \\ mm' + (mn' + nm')(\tfrac{1+\sqrt{D}}{2}) + &\ \underbrace{nn'(\tfrac{(1+D)+2\sqrt{D}}{4})}_{\frac{nn'(D-1)}{4} + nn'(\frac{1+\sqrt{D}}{2})}. \end{aligned}$$

Clearly closure holds $\iff 4 \mid D - 1 \iff D \underset{(4)}{\equiv} 1$. As we shall see, the "ring of integers" in $\mathbb{Q}[\sqrt{D}]$ is

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

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

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

$$R[x] := \{\text{sequences } (r_0, r_1, \ldots, r_n, \underbrace{0, 0, \ldots}_{\substack{\text{zero from} \\ \text{some point on}}}) \mid r_i \in R\}$$

and define, given $\underline{a} = (a_k)_{k\geq 0}$ and $\underline{b} = (b_k)_{k\geq 0}$,

$$\underline{a} + \underline{b} := (a_k + b_k)_{k\geq 0} \quad \text{and} \quad \underline{a} \cdot \underline{b} := (\textstyle\sum_{j=0}^{k} a_j b_{k-j})_{k\geq 0}.$$

Also put $0 := (0, 0, 0, \ldots)$ and $1 := (1, 0, 0, \ldots)$. Then we have

$$\begin{aligned}(\underline{a} + \underline{b}) \cdot \underline{c} &= (\textstyle\sum_{j=0}^{k} (a_j + b_j) c_{k-j}) \\ &= (\textstyle\sum_{j=0}^{k} a_j c_{k-j}) + (\textstyle\sum_{j=0}^{k} b_j c_{k-j}) = \underline{a} \cdot \underline{c} + \underline{b} \cdot \underline{c}\end{aligned}$$

and

$$\begin{aligned}(\underline{a} \cdot \underline{b}) \cdot \underline{c} &= (\textstyle\sum_{i=0}^{k} a_i b_{k-i}) \cdot \underline{c} = (\textstyle\sum_{\ell=0}^{k} (\textstyle\sum_{i=0}^{\ell} a_i b_{\ell-i}) c_{k-\ell}) \\ &\underset{\ell=i+j}{=} (\textstyle\sum_{i=0}^{k} a_i \textstyle\sum_{j=0}^{k-i} b_j c_{(k-i)-j}) = \underline{a} \cdot (\textstyle\sum_{j=0}^{k} b_j c_{k-j}) \\ &= \underline{a} \cdot (\underline{b} \cdot \underline{c}),\end{aligned}$$

so that II.A.1(iii) is satisfied.

Now identify R with the subring $\{(r, 0, 0, \ldots)\} \subset R[x]$. Taking $x := (0, 1, 0, 0, \ldots)$, we have $x^n = (\underbrace{0, \ldots, 0}_{n}, 1, 0, 0, \ldots)$ 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

$$R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])\,[x_n].$$

For any $r \in R$, we can consider the evaluation map

$$\mathrm{ev}_r \colon R[x] \longrightarrow R$$

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

$$\prod_{r\in R} \mathrm{ev}_r \colon R[x] \to \prod_{R} R \; (= \text{“}R^R\text{”})$$

of all such maps, sending a polynomial to (essentially) its “graph”. This is not always surjective (e.g. if $R = \mathbb{R}$) or injective (e.g. if $R = \mathbb{Z}_3$).

(v) Quaternions. The ring version is built out of the group one: put

$$\mathbb{H} := \{a + \mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\},$$

where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ have the same multiplicative properties as in the 8-element group 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 wth underlying set

$$M_n(R) := \{\textstyle\sum_{i,j=1}^n r_{ij}\mathbf{e}_{ij} \mid r_{ij} \in R\},$$

where the $\mathbf{e}_{ij}$ are formal symbols. Taking $A = \sum_{i,j} a_{ij}\mathbf{e}_{ij}$, $B = \sum_{i,j} b_{ij}\mathbf{e}_{ij}$, we set[2] $\mathbf{0} := \sum_{i,j=1}^n 0\mathbf{e}_{ij}$, $\mathbb{1} := \sum_{i,j=1}^n \delta_{ij}\mathbf{e}_{ij} = \sum_{i=1}^n \mathbf{e}_{ii}$, and

$$A + B := \sum_{i,j=1}^n (a_{ij} + b_{ij})\mathbf{e}_{ij} \quad \text{and} \quad AB := \sum_{i,j=1}^n (\textstyle\sum_{k=1}^n a_{ik}b_{kj})\mathbf{e}_{ij}.$$

Associativity follows from

$$(AB)C = \sum_{i,j=1}^n (\textstyle\sum_{k,\ell=1}^n a_{ik}b_{k\ell}c_{\ell j})\mathbf{e}_{ij} = A(BC)$$

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 $\mathbf{e}_{ij}$ as the matrix with a 1 at the $(i, j)^{\text{th}}$ place and zeroes elsewhere. We have

$$\mathbf{e}_{ij}\mathbf{e}_{k\ell} = \begin{cases} \mathbf{0}, & j \neq k \\ \mathbf{e}_{i\ell}, & j = k. \end{cases}$$

The noncommutativity is highly visible this way.

[2]Here δ_{ij} ($= 1$ if $i = j$, and 0 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** $\iff \exists\, r' \in R\backslash\{0\}$ 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 $\boxed{\left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right)} \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \mathbf{0}$, the boxed element is a left zero-divisor.
(ii) In $\boxed{\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)} \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) = \mathbf{0}$, the boxed element is nilpotent.
(iii) In $\boxed{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, 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 $\text{char}(R) = 0$.
(ii) $R = \mathbb{Z}_m$, $M_n(\mathbb{Z}_m)$, $\mathbb{Z}_m[x]$ have $\text{char}(R) = m$.
(iii) In a general *commutative* ring, we have

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{III.A.8}$$

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

$$(x+y)^p = x^p + y^p, \tag{III.A.9}$$

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 \\ & \ddots & \\ 0 & & r \end{pmatrix} = r\mathbb{1} = $ "r". More generally, $C(M_n(R)) = C(R)$.

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

$$\begin{aligned} \mathbf{0} = A\mathbf{e}_{k\ell} - \mathbf{e}_{k\ell}A &= \sum_{i,j=1}^{n} a_{ij}(\mathbf{e}_{ij}\mathbf{e}_{k\ell} - \mathbf{e}_{k\ell}\mathbf{e}_{ij}) \\ &= \sum_{i=1}^{n} a_{ik}\mathbf{e}_{i\ell} - \sum_{j=1}^{n} a_{\ell j}\mathbf{e}_{kj}. \end{aligned}$$

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

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.[4]

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 $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Another example is $M_n(\mathbb{R})^* = \mathrm{GL}_n(\mathbb{R})$, which everyone knows is the matrices with determinant in $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$. 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 $\begin{pmatrix} \mathbf{k} & 1 \\ \mathbf{j} & \mathbf{i} \end{pmatrix} \in M_2(\mathbb{H})$. The "determinant" $\mathbf{ki} - 1\mathbf{j} = \mathbf{j} - \mathbf{j} = 0$, but

$$\begin{pmatrix} \mathbf{k} & 1 \\ \mathbf{j} & \mathbf{i} \end{pmatrix} \begin{pmatrix} -\frac{\mathbf{k}}{2} & -\frac{\mathbf{j}}{2} \\ \frac{1}{2} & -\frac{\mathbf{i}}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1}.$$

[4]In Jacobson, R^* means $R\backslash\{0\}$, and $U(R)$ is the group of units. We will not use this notation; the notation given above is more standard.

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

$$\text{(III.A.14)} \qquad \begin{array}{rcl} \mathbb{Z} \times \mathbb{Z}_2 & \cong & \left(\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]\right)^* \\ (a, \pm 1) & \mapsto & \pm\left(\frac{1+\sqrt{5}}{2}\right)^a. \end{array}$$

Given $\alpha = \frac{x+y\sqrt{5}}{2} \in R := \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, 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 $(\alpha\tilde{\alpha})(\alpha'\tilde{\alpha}') = \alpha\alpha'\widetilde{\alpha\alpha'} = 1\tilde{1} = 1$. Since $x \underset{(2)}{\equiv} y$, we have that $x^2 \underset{(4)}{\equiv} 5y^2 \implies \alpha\tilde{\alpha} = \frac{x^2-5y^2}{4} \in \mathbb{Z}$, and similarly for $\alpha'\tilde{\alpha}'$. So the only way the product of $\alpha\tilde{\alpha}$ and $\widetilde{\alpha\alpha'}$ is 1, is if they are both ± 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,[5]

$$\text{(III.A.15)} \qquad \mathcal{O}_K^* \cong \mathbb{Z}^{r_1+r_2-1} \times \{\text{torsion group}\},$$

where $\mathcal{O}_K \subset K$ 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.

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