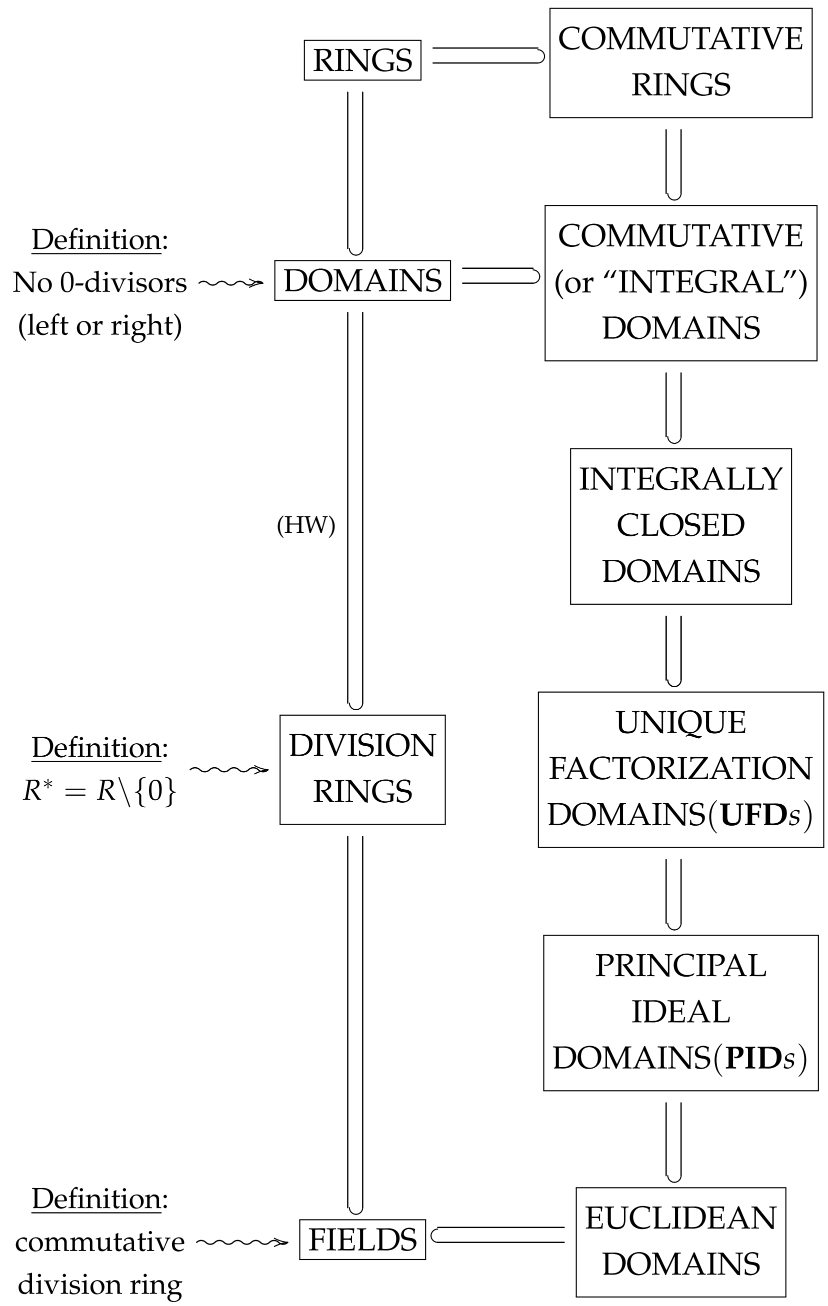
III.B. Ring zoology

(III.B.1)



We will define integrally closed domains, UFDs (also called "Factorial" domains) and PIDs later.

III.B.2. DEFINITION. A **Euclidean domain** is a commutative domain which has a function

$$\delta\colon R\backslash\{0\} \to \mathbb{N}$$

with the following property: for all $a \in R$ and $b \in R\backslash\{0\}$, there exist $q, r \in R$ satisfying $a = bq + r$ and either $\delta(r) < \delta(b)$ or $r = 0$. (This δ is called a *Euclidean function* and is not unique.)

Clearly, these are just the domains to which we can generalize the (Euclidean) division algorithm I.B.3.

III.B.3. REMARK. The best choice for δ, when possible, is to have $\delta(1) = 1$ and $\delta^{-1}(1) = R^*$. This will be the case in all examples below.

In the remainder of the section I simply comment on some of the inclusions in (III.B.1) and give a few examples.

III.B.4. EXAMPLE. Given $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}\backslash\{0\}$, set $\bar{\alpha} := a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. We have

$$\alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2 + ab(-\mathbf{i} + \mathbf{i}) + ac(-\mathbf{j} + \mathbf{j}) + ad(-\mathbf{k} + \mathbf{k}) \\ + bc(-\mathbf{ij} - \mathbf{ji}) + bd(-\mathbf{ik} - \mathbf{ki}) + cd(-\mathbf{jk} - \mathbf{kj})$$

$\implies \frac{\bar{\alpha}}{a^2+b^2+c^2+d^2} = \alpha^{-1}$. This proves that

noncommutative division rings exist.

III.B.5. EXAMPLE. $\mathbb{Z}_6$ firnishes an example of a commutative ring which is not a domain, due to the (obviously non-invertible) zero-divisors $\bar{2}$, $\bar{3}$, and $\bar{4}$.

III.B.6. PROPOSITION. *Given a field $\mathbb{F}$, (a) $\mathbb{F}$ and (b) $\mathbb{F}[x]$ are Euclidean domains.*[6]

[6] As will be seen very easily later, $\mathbb{F}[x, y]$ is non-Euclidean.

PROOF. (a) Put $\delta(r) := 1\ \forall r \in \mathbb{F}\backslash\{0\}$. Set $q = b^{-1}a$, $r = 0$.
(b) Put $\delta(P(x)) := 2^{\deg(P(x))}$. Use polynomial long division to construct q, r. □

III.B.7. EXAMPLE. $\mathbb{Q}[\mathbf{i}]$ is a field. (Here, and elsewhere, $\mathbf{i} := \sqrt{-1}$.) To see this, simply write

$$\frac{1}{a+b\mathbf{i}} = \frac{a-b\mathbf{i}}{(a+b\mathbf{i})(a-b\mathbf{i})} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\mathbf{i}.$$

Similarly, we can show $\mathbb{Q}[\sqrt{d}]$ is a field for any $d \in \mathbb{Z}$.

III.B.8. PROPOSITION. *(a) $\mathbb{Z}$ and (b) $\mathbb{Z}[\mathbf{i}]$ are Euclidean domains.*

PROOF. (a) Put $\delta(m) := |m|$ and use the division algorithm.
(b) Writing $\alpha = a + b\mathbf{i}$, put $\delta(\alpha) := \alpha\bar{\alpha} = |\alpha|^2 = a^2 + b^2$. Let $\alpha \in \mathbb{Z}[\mathbf{i}]$ and $\beta \in \mathbb{Z}[\mathbf{i}]\backslash\{0\}$. We will find μ and ρ in $\mathbb{Z}[\mathbf{i}]$ such that $\alpha = \beta\mu + \rho$ and $\delta(\beta) > \delta(\rho)$.

Working in $\mathbb{Q}[\mathbf{i}]$, we have $\alpha\beta^{-1} = x + y\mathbf{i}$; pick $m, n \in \mathbb{Z}$ such that $\epsilon := x - m$ and $\eta := y - n$ have $|\epsilon|, |\eta| \leq \frac{1}{2}$. Then

$$\alpha = \beta\{(m+\epsilon) + (n+\eta)\mathbf{i}\} = \beta\{\underbrace{m + n\mathbf{i}}_{=:\mu}\} + \underbrace{\beta\{\epsilon + \eta\mathbf{i}\}}_{=:\rho}.$$

Clearly $\mu \in \mathbb{Z}[\mathbf{i}]$, and so $\rho = \alpha - \beta\mu \in \mathbb{Z}[\mathbf{i}]$ also. Now

$$\begin{aligned}\delta(\rho) = |\rho|^2 = |\beta|^2|\epsilon + \eta\mathbf{i}|^2 &= \delta(\beta)\{\epsilon^2 + \eta^2\} \\ &\leq \delta(\beta) \cdot \{\tfrac{1}{4} + \tfrac{1}{4}\} < \delta(\beta),\end{aligned}$$

and we are done. □

III.B.9. REMARK. The δ in the proof of (b) is an example of a *Galois norm*. This is easy to generalize to quadratic number rings $R = \mathbb{Z}[\sqrt{D}]$ and (if $D \underset{(4)}{\equiv} 1$) $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Given $\alpha = a + b\sqrt{D}$, write $\tilde{\alpha} := a - b\sqrt{D}$ (which is the complex conjugate $\bar{\alpha}$ if $D < 0$); then we define the norm by $\mathcal{N}(\alpha) := \alpha\tilde{\alpha}$. When this gives a Euclidean function, a number ring is called *norm-Euclidean*. For imaginary quadratic ($D < 0$), in which case Euclidean and norm-Euclidean are equivalent, the complete list is

$$\mathbb{Z}[\sqrt{-1}],\ \mathbb{Z}[\sqrt{-2}],\ \mathbb{Z}[\tfrac{1+\sqrt{-3}}{2}],\ \mathbb{Z}[\tfrac{1+\sqrt{-7}}{2}],\ \text{and}\ \underbrace{\mathbb{Z}[\tfrac{1+\sqrt{-11}}{2}]}_{\text{(HW)}}.$$

In the real quadratic case, the list of norm-Euclidean cases is much longer (but finite) and strictly smaller than the list of Euclidean cases (which is conjectured to be infinite).

We should also mention that for a ring R,

$$\text{(III.B.10)} \quad R \text{ is a domain} \iff \left(\left\{ \begin{array}{c} ab = ac \text{ or } ba = ca \\ \text{AND} \\ a \neq 0 \end{array} \right\} \implies b = c \right).$$

PROOF. If R is a domain, suppose $a(b-c) = 0$ with $a \neq 0$; then as there are no zero-divisors, $b - c = 0$.

Conversely, assume the condition on RHS(III.B.10), and suppose $ab = 0$ with $a \neq 0$. Then $ab = a0 \implies b = 0$, and no left zero-divisors exist. (Now reverse a and b.) □

Finally, note that

$$\text{(III.B.11)} \qquad R \text{ is a domain} \implies \text{char}(R) \text{ is prime or } 0.$$