Ring basics

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/

28 February, 2024 (at *19:02*)

Semigroups & Monoids.

A ***semigroup*** is a pair $(S, \bullet)$, where $\bullet$ is an associative *binary operation* [***binop***] on set S. A special case is a ***monoid***. It is a triple $(S, \bullet, \mathbf{e})$, where $\bullet$ is an associative binop on S, and $\mathbf{e} \in S$ is a two-sided identity elt.

Axiomatically:

G1: Binop $\bullet$ is ***associative***, i.e $\forall\alpha,\beta,\gamma \in S$, necessarily $[\alpha \bullet \beta] \bullet \gamma = \alpha \bullet [\beta \bullet \gamma]$.

G2: Elt $\mathbf{e}$ is a ***two-sided identity element***, i.e $\forall\alpha \in S$: $\alpha \bullet \mathbf{e} = \alpha$ and $\mathbf{e} \bullet \alpha = \alpha$.

Moreover, we call S a ***Group*** if t.fol also holds.

G3: Each elt admits a ***two-sided inverse element***: $\forall\alpha$, $\exists\beta$ such that $\alpha \bullet \beta = \mathbf{e}$ and $\beta \bullet \alpha = \mathbf{e}$.

When the binop is '+', *addition*, then write the inverse of α as $-\alpha$ and call it "***negative*** α". We then use 0 for the id-elt.

When the binop is '*multiplication*', write the inverse of α as α^{-1} and call it the "***reciprocal*** of α" We use 1 for the id-elt. Usually, one omits the binop-symbol and writes $\alpha\beta$ for $\alpha \bullet \beta$.

For an *abstract* binop '$\bullet$', we often write α^{-1} for the inverse of α ["α inverse"], and omit the binop-symbol. If $\bullet$ is ***commutative*** [$\forall\alpha,\beta$, necessarily $\alpha \bullet \beta = \beta \bullet \alpha$] then we call S a ***commutative group***.

Rings/Fields.

A ***ring*** is a five-tuple $(\Gamma, +, 0, \cdot, 1)$ with these axioms.

R1: Elements 0 and 1 are distinct; $0 \neq 1$.

R2: Triple $\big(\Gamma, +, 0\big)$ is a commutative group.

R3: Triple $\big(\Gamma, \cdot, 1\big)$ is monoid.

R4: Mult. ***distributes-over*** addition from the *left*, $\alpha[x + y] = [\alpha x] + [\alpha y]$, and from the *right*, $[x + y]\alpha = [x\alpha] + [y\alpha]$; this, for all $\alpha, x, y \in \Gamma$.

Our Γ is a ***commutative ring*** (abbrev.: ***commRing***) if the multiplication is commutative.

When Γ is commutative: Say that $\alpha \bullet\!\mid \beta$ [α ***divides*** β] if *there exists* $\mu \in \Gamma$ s.t $\alpha\mu = \beta$. This is the same relation as $\beta \mid\!\bullet\, \alpha$ [β is a multiple of α].

Zero-divisors.

Fix $\alpha \in \Gamma$. Elt $\beta \in \Gamma$ is a "**(*two-sided*) *annihilator*** of α" if $\alpha\beta = 0 = \beta\alpha$. An α is a **(*two-sided*) *zero-divisor*** if it admits a *non-zero* annihilator. So 0 is a ZD, since $0 \cdot 1 = 0 = 1 \cdot 0$, and $1 \neq 0$. We write the *set* of Γ–zero-divisors as

$$\mathrm{ZD}_\Gamma \quad \text{or} \quad \mathrm{ZD}(\Gamma)\,.$$

[E.g: In the $\mathbb{Z}_{15}$ ring, note $9 \not\equiv 0$ and $10 \not\equiv 0$, yet $9 \cdot 10$ *is* $\equiv 0$. So each of 9 and 10 is a "*non-trivial zero-divisor* in $\mathbb{Z}_{15}$".]

An $\alpha \in \Gamma$ is a Γ-***unit*** if $\exists\beta \in \Gamma$ st. $\alpha\beta = 1 = \beta\alpha$. Use

$$\mathbf{U}_\Gamma \quad \text{or} \quad \mathbf{U}(\Gamma)$$

for the units group. In the special case when Γ is $\mathbb{Z}_N$, I will write Φ_N for its units group, to emphasize the relation with the Euler-phi fnc, since $\varphi(N) := |\Phi_N|$. [Some texts use $\mathbf{U}(N)$ for the $\mathbb{Z}_N$ units group.]

Integral domains, Fields.

A ***commutative ring*** is a ring in which the multiplication is commutative. A commRing with no (non-zero) zero-divisors [that is, $\mathrm{ZD}_\Gamma = \{0\}$] is called an ***integral domain*** (***intDomain***), or sometimes just a ***domain***.

An intDomain F in which every non-zero element is a unit [i.e $\mathbf{U}(F) = F \smallsetminus \{0\}$] is a ***field***. That is to say, F is a commRing where triple $(F \smallsetminus \{0\}, \cdot, 1)$ is a group.

Examples. The fields we know are: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and, for p prime, $\mathbb{Z}_p$.

Every ring has the "trivial zero-divisor" —zero itself. The ring of integers doesn't have others. In contrast, the non-trivial zero-divisors of $\mathbb{Z}_{12}$ comprise $\{\pm 2, \pm 3, \pm 4, 6\}$.

In $\mathbb{Z}$ the units are ± 1. But in $\mathbb{Z}_{12}$, the ring of integers mod-12, the set of units, $\Phi(12)$, is $\{\pm 1, \pm 5\}$. In the ring $\mathbb{Q}$ of rationals, *each* non-zero element is a unit. In the ring $\mathbb{G} := \mathbb{Z} + \mathbf{i}\mathbb{Z}$ of ***Gaussian integers***, the units group is $\{\pm 1, \pm \mathbf{i}\}$. [Aside: Units($\mathbb{G}$) is cyclic, generated by $\mathbf{i}$. And Units($\mathbb{Z}_{12}$) is not cyclic. For which N is $\Phi(N)$ cyclic?] □

Irreducibles, Primes. Consider $(\Gamma, +, 0, \cdot, 1)$, a commutative ring[♡1]. An elt $\alpha \in \Gamma$ is a ***zero-divisor*** [abbrev **ZD**] if there exists a *non-zero* $\beta \in \Gamma$ st. $\alpha\beta = 0$.

In contrast, an element $u \in \Gamma$ is a ***unit*** if $\exists w \in \Gamma$ st. $u\cdot w = 1$. This w, written as u^{-1}, is called the ***reciprocal*** [or ***multiplicative-inverse***] of u. [When an element *has* a mult-inverse, this mult-inverse is unique.]

Exer 1a: If α divides a unit, $\alpha \bullet\!| \; u$, then α is a unit.

Exer 1b: If $\gamma \;|\!\bullet z$ with $z \in$ ZD, then γ is a zero-divisor.

Exer 2: In an arbitrary ring Γ, the set ZD(Γ) is *disjoint* from Units(Γ).

An element $p \in \Gamma$ is:

i: Γ-***irreducible*** if p is a non-unit, non-ZD, such that for each Γ-factorization $p = x\cdot y$, either x or y is a Γ-unit. [Restating, using the definition below: Either $x \approx 1, y \approx p$, or $x \approx p, y \approx 1$.]

ii: Γ-***prime*** if p is a non-unit, non-ZD, such that for each pair $c,d \in \Gamma$: If $p \bullet\!| \; [c\cdot d]$ then *either* $p \bullet\!| \; c$ or $p \bullet\!| \; d$.

Associates. In a *commutative* ring, elts α and β are ***associates***, written $\alpha \approx \beta$, if *there exists* a unit u st. $\beta = u\alpha$. [For emphasis, we might say ***strong associates***.] They are ***weak-associates***, written $\alpha \sim \beta$, if $\alpha \bullet\!| \; \beta$ *and* $\alpha \;|\!\bullet \beta$ [i.e, $\alpha \in \beta\Gamma$ and $\beta \in \alpha\Gamma$].

Ex 3: Prove *Assoc $\Rightarrow$ weak-Assoc.*

Ex 4: If $\alpha \sim \beta$ and $\alpha \notin$ ZD, then α, β are (strong) associates.

Ex 5: In $\mathbb{Z}_{10}$, zero-divisors $2, 4$ *are* weak-associates. [This, since $2\cdot 2 \equiv 4$ and $4\cdot 3 = 12 \equiv 2$.] Are $2, 4$ (strong) associates?

Ex 6: With $d \bullet\!| \; \alpha$, prove: *If α is a non-ZD, then d is a non-ZD.* And: *If α is a unit, then d is a unit.*

1: Lemma. *In a commRing[♡1] Γ, each prime $\boldsymbol{\alpha}$ is irreducible.* ◊

Proof. Consider factorization $\boldsymbol{\alpha} = xy$. Since $\boldsymbol{\alpha} \bullet\!| \; xy$, WLOG $\boldsymbol{\alpha} \bullet\!| \; x$, i.e $\exists c$ with $\boldsymbol{\alpha}c = x$. Hence

$$*: \qquad \boldsymbol{\alpha} = xy = \boldsymbol{\alpha}cy\,.$$

By defn, $\boldsymbol{\alpha} \notin$ ZD. We may thus cancel in $(*)$, yielding $1 = cy$. So y is a unit. ♦

There are rings[♡2] with irreducible elements p which are nonetheless not prime. However…

2: Lemma. *Suppose commRing Γ satisfies the Bézout condition, that each GCD is a linear-combination. Then each irreducible $\boldsymbol{\alpha}$ is prime.* ◊

Pf. Suppose $\boldsymbol{\alpha} \bullet\!| \; c\cdot d$. WLOG $\boldsymbol{\alpha} \bullet\!\nmid c$. Let $g := \text{GCD}(\boldsymbol{\alpha}, c)$. Were $g \approx \boldsymbol{\alpha}$, then $\boldsymbol{\alpha} \bullet\!| \; g \bullet\!| \; c$, a contradiction. Thus, since $\boldsymbol{\alpha}$ is irreducible, our $g \approx 1$.

Bézout produces $S,T \in \Gamma$ with

$$1 = S\boldsymbol{\alpha} + Tc\,. \quad \textit{Hence}$$

$$*: \qquad d = S\boldsymbol{\alpha}d + Tcd = Sd\boldsymbol{\alpha} + Tcd\,.$$

By hyp, $\boldsymbol{\alpha} \bullet\!| \; cd$, hence $\boldsymbol{\alpha}$ divides RhS$(*)$. So $\boldsymbol{\alpha} \bullet\!| \; d$. ♦

3: Lemma. *In commRing Γ, if prime p divides product $\alpha_1 \cdots \alpha_K$ then $p \bullet\!| \; \alpha_j$ for some j.* [*Exer. 7*] ◊

4: Prime-uniqueness thm. *In commRing Γ, suppose*

$$p_1\cdot p_2\cdot p_3 \cdots p_K = q_1\cdot q_2\cdot q_3 \cdots q_L$$

are equal products-of-primes. Then $L = K$ and, after permuting the p primes, each $p_k \approx q_k$. ◊

Pf. [From Ex.4, previously, for non-ZD, relations $\sim$ and $\approx$ are the same.] For notational simplicity, we do this in $\mathbb{Z}_+$, in which case $p_k \approx q_k$ will be replaced by $p_k = q_k$.

FTSOC, consider a CEX which minimizes sum $K+L$; necessarily positive. WLOG $L \geq 1$. Thus $K \geq 1$. [Otherwise, q_L divides a unit, forcing q_L to be a unit; see Ex.1a.] By the preceding lemma, q_L divides *some* p_k; WLOG $q_L \bullet\!| \; p_K$. Thus $q_L = p_K$ [since p_K is prime and q_L is not a unit]. Cancelling now gives $p_1\cdot p_2 \cdots p_{K-1} = q_1\cdot q_2 \cdots q_{L-1}$, giving a CEX with a *smaller* $[K-1]+[L-1]$ sum. ♦

[♡1] More generally, a commutative monoid.

[♡2] Consider the ring, Γ, of polys with coefficients in $\mathbb{Z}_{12}$. There, $x^2 - 1$ factors as $[x-5][x+5]$ *and* as $[x-1][x+1]$. Thus none of the four linear terms is prime. Yet each is Γ-irreducible. (Why?) This ring Γ has zero-divisors (yuck!), but there are natural subrings of $\mathbb{C}$ where Irred$\not\Rightarrow$Prime.

Example where $\sim \neq \approx$. Here a modification of an example due to Irving ("Kap") Kaplansky.

Let Ω be the ring of real-valued *continuous* fncs on $[-2,2]$. Define $\mathcal{E},\mathcal{D} \in \Omega$ by: *For* $t \geq 0$:

$$\mathcal{E}(t) \;=\; \mathcal{D}(t) \;:=\; \begin{Bmatrix} t-1 & \text{if } t\in[1,2] \\ 0 & \text{if } t\in[0,1] \end{Bmatrix}.$$

And for $t \leq 0$ define

$$\mathcal{E}(t) \;:=\; \mathcal{E}(-t) \quad \textit{and} \quad \mathcal{D}(t) \;:=\; -\mathcal{D}(-t)\,.$$

[So $\mathcal{E}$ is an Even fnc; $\mathcal{D}$ is odD.] Note $\mathcal{E} = f\mathcal{D}$ and $\mathcal{D} = f\mathcal{E}$, where

$$f(t) \;:=\; \begin{Bmatrix} 1 & \text{if } t\in[1,\,2] \\ t & \text{if } t\in[-1,\,1] \\ -1 & \text{if } t\in[-2,-1] \end{Bmatrix}.$$

Hence $\mathcal{E} \sim \mathcal{D}$. [This f is not a unit, since $f(0)=0$ has no reciprocal. However, f is a *non*-ZD: For if $fg = \mathbf{0}$, then g must be zero on $[-2,2] \smallsetminus \{0\}$. Cty of g then forces $g \equiv \mathbf{0}$.]

Could there be a unit $u \in \Omega$ with $u\mathcal{D} = \mathcal{E}$? Well

$$u(2) = \frac{\mathcal{E}(2)}{\mathcal{D}(2)} \overset{\text{note}}{=\!=} +1\,, \quad \textit{and} \quad u(-2) = \frac{\mathcal{E}(-2)}{\mathcal{D}(-2)} \overset{\text{note}}{=\!=} -1\,.$$

Cty of $u()$ forces u to be zero somewhere on interval $(-2,2)$, hence u is *not* a unit. □

Addendum. By Ex.4, both $\mathcal{E}$ and $\mathcal{D}$ must be zero-divisors. [Exer.8: Exhibit a function $g \in \Omega$, *not* the zero-fnc, such that $\mathcal{E}\cdot g \equiv \mathbf{0}$.] □