Ring basics

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
3 October, 2018 (at *09:01*)

Semigroups. For us, a ***semigroup*** is a triple $(S, \bullet, \mathbf{e})$, where $\bullet$ is an associative binary operation on set S, and $\mathbf{e} \in S$ is a two-sided identity elt.[♡1]

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 '+', then we write the inverse of α as $-\alpha$ and call it "***negative*** α".

If we refer to the binop as 'multiplication' then write the inverse of α as α^{-1} and call it "the ***reciprocal*** of α". Also, we usually omit the binop-symbol and write $\alpha\beta$ for $\alpha \cdot \beta$.

For an abstract binop '$\bullet$', we usually write α^{-1} for the inverse of α, and we call it "α inverse". If $\bullet$ is ***commutative*** [$\forall \alpha,\beta$, necessarily $\alpha \bullet \beta = \beta \bullet \alpha$] then we call S a ***commutative (semi)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 semigroup.

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 $\alpha,x,y \in \Gamma$.

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

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

An $\alpha \in \Gamma$ is a Γ-***unit*** if $\exists \beta \neq 0$ st. $\alpha\beta = 1 = \beta\alpha$. Use

$$\mathrm{Units}_\Gamma \quad \text{or} \quad \mathrm{Units}(\Gamma)$$

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

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

An intDomain F in which every non-zero element is a unit, $\mathrm{Units}(F) = F \smallsetminus \{0\}$, is a ***field***. I.e, F is a commRing such that triple $\Big(F \smallsetminus \{0\},\ \cdot\ ,\ 1\Big)$ is a group.

Examples. 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 $\mathbb{G} := \mathbb{Z} + i\mathbb{Z}$ of ***Gaussian integers***, the units group is $\{\pm 1, \pm i\}$. [Aside: $\mathrm{Units}(\mathbb{G})$ is cyclic, generated by i. And $\mathrm{Units}(\mathbb{Z}_{12})$ is not cyclic. For which N is $\Phi(N)$ cyclic?] □

[♡1] What I'm calling a semigroup is usually called a ***monoid***. The std defn of ***semigroup*** does not require an identity-elt.

Irreducibles, Primes. Consider a commutative ring $(\Gamma, +, 0, \cdot, 1)$. 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 is the "multiplicative inverse" of u, is unique, and is often written u^{-1}.) Exer 1: In an arbitrary ring Γ, the set ZD(Γ) is *disjoint* from Units(Γ).

An element α is:

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

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

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

Ex 2: Prove *Strong-Assoc* $\Rightarrow$ *Assoc.*

Ex 3: If $\alpha \sim \beta$ and $\alpha \notin$ ZD, then α, β are **strong** associates.

Ex 4: In $\mathbb{Z}_{10}$, zero-divisors $2, 4$ *are* associates. Are they strong associates?

Ex 5: 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 Γ, each prime α is irreducible.* ◊

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

$$*: \qquad \alpha \ = \ xy = \alpha cy \, .$$

By defn, $\alpha \notin$ 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] 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.

2: Lemma. *Suppose commRing Γ satifies the Bézout condition, that each GCD is a linear-combination. Then each irreducible α is prime.* ◊

Proof. Suppose $\alpha \bullet\!\!| \ xy$ and WLOG $\alpha \not\bullet\!\!| \ x$. Let $g := \text{GCD}(\alpha, x)$. Were $g \approx \alpha$, then $\alpha \bullet\!\!| \ g \bullet\!\!| \ x$, a contradiction. Thus, since α is irreducible, our $g \approx 1$.

Bézout produces S,$T \in \Gamma$ with

$$1 \ = \ S\alpha + Tx \, . \quad \textit{Hence}$$
$$*: \qquad y \ = \ S\alpha y + Txy \ = \ Sy\alpha + Txy \, .$$

By hyp, $\alpha \bullet\!\!| \ xy$, hence α divides RhS$(*)$. So $\alpha \bullet\!\!| \ y$. ♦

Example where $\sim \neq \approx$. Here a modification of an example due to Kaplansky.

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

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

And for $t \leqslant 0$ 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 $g = \mathbf{0}$.]

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

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

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