Ring basics

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
13 July, 2016 (at *00:54*)

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 $(\mathbf{\Gamma}, +, 0, \cdot, 1)$ with these axioms.

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

R2: Triple $\left(\mathbf{\Gamma}, +, 0\right)$ is a commutative group.

R3: Triple $\left(\mathbf{\Gamma} \setminus \{0\}, \cdot, 1\right)$ 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 $\alpha,x,y \in \mathbf{\Gamma}$.

If the multiplication is commutative then $\mathbf{\Gamma}$ is a ***commutative ring***.

Fix $\alpha \in \mathbf{\Gamma}$. Elt $\beta \in \mathbf{\Gamma}$ 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 $\mathbf{\Gamma}$–zero-divisors as

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

A *commutative* ring with no (non-zero) zero-divisors [i.e $\mathrm{ZD}_{\mathbf{\Gamma}} = \{0\}$] is called an ***integral domain***, or sometime just a ***domain***.

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

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

for the units group. In the special case when $\mathbf{\Gamma}$ 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 $\varphi(N) := |\Phi_N|$.

Fields. A ***field*** F is a *commutative ring* such that triple $\left(F \setminus \{0\}, \cdot, 1\right)$ is a group. In other words, $\mathrm{Units}(F) = F \setminus \{0\}$.

[♡1] What I'm calling a semigroup is usually called a ***monoid***.