Ring basics

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
6 July, 2018 (at *11:12*)

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 $\alpha,x,y \in \mathbf{\Gamma}$.

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

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

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 $\varphi(N) := |\Phi_N|$.

Characteristic of a ring. In a ring $(\mathbf{\Gamma}, +, \mathbf{0}, \cdot, \mathbf{1})$, if there is a posint n so that $\mathbf{1} + \mathbf{1} + \overset{n}{\cdots} + \mathbf{1}$ equals $\mathbf{0}$, then the *smallest* such n is called the "***characteristic*** of $\mathbf{\Gamma}$", written as $\mathrm{Char}(\mathbf{\Gamma}) = n$. If no such posint exists, then it would make sense to write $\mathrm{Char}(\mathbf{\Gamma}) = \infty$; however, the *standard term* is $\mathrm{Char}(\mathbf{\Gamma}) = 0$. As examples, $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$ each have characteristic zero, whereas $\mathbb{Z}_6$ has characteristic 6. (As does $\mathbb{Z}_6[\![x]\!]$, the ring of polynomials with coeffs from $\mathbb{Z}_6$.)

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 $\mathrm{ZD}_{\mathbf{\Gamma}} = \{0\}$] is called an ***integral domain***, [***intDomain***] or sometimes just a ***domain***.

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

Irreducibles, Primes. Consider a commutative ring $(\mathbf{\Gamma}, +, 0, \cdot, 1)$. An elt $\alpha \in \mathbf{\Gamma}$ is a ***zero-divisor*** (abbrev **ZD**) if there exists a *non-zero* $\beta \in \mathbf{\Gamma}$ st. $\alpha\beta = 0$. In contrast, an element $u \in \mathbf{\Gamma}$ is a ***unit*** if $\exists w \in \mathbf{\Gamma}$ st. $u \cdot w = 1$. (This w is the "multiplicative inverse" of u, is unique, and is often written u^{-1}.) Exer: In an arbitrary ring $\mathbf{\Gamma}$, the set $\mathrm{ZD}(\mathbf{\Gamma})$ is *disjoint* from $\mathrm{Units}(\mathbf{\Gamma})$.

An element α is:

i: ***$\mathbf{\Gamma}$-irreducible*** if α is a non-unit, non-ZD, such that for each $\mathbf{\Gamma}$-factorization $\alpha = x \cdot y$, either x or y is a $\mathbf{\Gamma}$-unit.

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

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

Two ring-elements α and β are ***associates***, written $\alpha \overset{\text{as}}{\sim} \beta$, if $\alpha \bullet\!\!| \ \beta$ *and* $\alpha \ |\!\!\bullet \ \beta$ [i.e, $\alpha \in \beta\mathbf{\Gamma}$ and $\beta \in \alpha\mathbf{\Gamma}$]. They are ***strong associates*** if there exists a unit u st. $\beta = u\alpha$. Exer: Prove *Strong-Assoc* $\Rightarrow$ *Assoc.*

Exer: Ring $\mathbb{Z}_N$ has no irreducible elements, since $\mathbb{Z}_N$ is the disjoint-union ZD $\sqcup$ Units.

Exer: PRIME$\Rightarrow$IRRED. However there are rings[♡2] with irreducible elements p which are nonetheless not prime.

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: Units($\mathbb{G}$) is cyclic, generated by i. And Units($\mathbb{Z}_{12}$) is not cyclic. For which N is $\Phi(N)$ cyclic?] □

NB: Later pages are not necessary for our course, and are not proofread.

Whoa! These notes are in-progress, and not yet proofread.

Intro to Ideals of a commutative ring

Henceforth, $\mathbf{\Gamma}$ is a commRing. An ***ideal*** $\boldsymbol{\mathcal{I}} \subset \mathbf{\Gamma}$ is an additive-subgroup st. $\forall x \in \mathbf{\Gamma}$, necessarily $x\boldsymbol{\mathcal{I}} \subset \boldsymbol{\mathcal{I}}$. The two trivial ideals are the ***zero-ideal*** $\{0\}$, and $\mathbf{\Gamma}$.

The "***radical*** of $\boldsymbol{\mathcal{I}}$" is

1.1: $$\sqrt{\boldsymbol{\mathcal{I}}} \ := \ \left\{ \alpha \in \mathbf{\Gamma} \ \middle| \ \exists \mathcal{K} \in \mathbb{Z}_+ \text{ with } \alpha^{\mathcal{K}} \in \boldsymbol{\mathcal{I}} \right\}.$$

Let $\text{Deg}_{\boldsymbol{\mathcal{I}}}(\alpha)$ denote the smallest such $\mathcal{K}$.

1.2: Lemma. *The radical $\sqrt{\boldsymbol{\mathcal{I}}}$ is itself an ideal.* ♢

Proof. With $\alpha \in \sqrt{\boldsymbol{\mathcal{I}}}$ of $\boldsymbol{\mathcal{I}}$-degree $\mathcal{K}$, and arbitrary $x \in \mathbf{\Gamma}$, note that $[\alpha x]^{\mathcal{K}} = \alpha^{\mathcal{K}} x^{\mathcal{K}}$ is in $\boldsymbol{\mathcal{I}}$, since $\alpha^{\mathcal{K}} \in \boldsymbol{\mathcal{I}}$. Hence $\alpha x \in \sqrt{\boldsymbol{\mathcal{I}}}$.

Fix elements α,β of $\boldsymbol{\mathcal{I}}$-degrees $\mathcal{K}$,$\mathcal{L}$. The Binomial Thm says that $[\alpha + \beta]^{\mathcal{K}+\mathcal{L}}$ is a sum of

$$\text{coefficient–times–}\alpha^k\beta^\ell \text{ terms},$$

where $k + \ell = \mathcal{K} + \mathcal{L}$. Necessarily, either $k \geqslant \mathcal{K}$, so $\boldsymbol{\mathcal{I}} \ni \alpha^k$, or else $\ell \geqslant \mathcal{L}$, whence $\boldsymbol{\mathcal{I}} \ni \beta^\ell$,. In either case, $\boldsymbol{\mathcal{I}}$ owns this coefficient-times-$\alpha^k\beta^\ell$ term. Thus

$$\boldsymbol{\mathcal{I}} \ni [\alpha + \beta]^{\mathcal{K}+\mathcal{L}} \quad \text{so} \quad \sqrt{\boldsymbol{\mathcal{I}}} \ni \alpha + \beta \,. \qquad \blacklozenge$$

Nilpotent elements. Element $\nu \in \mathbf{\Gamma}$ is ***nilpotent*** if $\exists \mathcal{K} \in \mathbb{Z}_+$ such that $\nu^{\mathcal{K}} = 0$. The smallest such $\mathcal{K}$ is the "***nilpotency degree*** of ν", written NilDeg(ν); remark that ν is a zero-divisor, since $\nu^{\mathcal{K}-1} \neq 0$, yet $0 = \nu^{\mathcal{K}-1} \cdot \nu$.

The *set* $\boldsymbol{\mathcal{N}}_{\mathbf{\Gamma}}$ of nilpotent elements is called the "***nil-radical*** of $\mathbf{\Gamma}$". Evidently:

1.3: *The nilradical,* $\boldsymbol{\mathcal{N}}_{\mathbf{\Gamma}} \overset{\text{note}}{=\!=} \sqrt{\{0\}}$, *is an ideal.*

1.4: Lemma. *In $\mathbf{\Gamma}$, consider a unit u and nilpotent ν. Then $u + \nu$ and $u - \nu$ are units.* ♢

Proof. ISTShow $u - \nu$ a unit. Element $\delta := u^{-1}\nu$ is nilpotent, since $\boldsymbol{\mathcal{N}}_{\mathbf{\Gamma}}$ is an ideal. Note $u - \nu$ equals $u \cdot [1 - \delta]$, so ISTShow that $1 - \delta$ is a unit. Define $\mathcal{K} := \text{NilDeg}(\delta)$ and

$$\sigma \ := \ 1 + \delta + \delta^2 + \ldots + \delta^{\mathcal{K}-1} \,.$$

Finally, $[1 - \delta] \cdot \sigma = 1 - \delta^{\mathcal{K}} \overset{\text{note}}{=\!=} 1$. ♦

[♡2] Consider the ring, $\mathbf{\Gamma}$, 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 $\mathbf{\Gamma}$-irreducible. (Why?) This ring $\mathbf{\Gamma}$ has zero-divisors (yuck!), but there are natural subrings of $\mathbb{C}$ where Irred$\not\Rightarrow$Prime.

Polynomial rings

Here, $\mathbf{R}$ is a commutative ring (possibly with zero-divisors) and $\mathbf{\Gamma} := \mathbf{R}[\![\mathsf{z}]\!]$ is its polynomial ring. We regard $\mathbf{\Gamma}$ as a ring-extension $\mathbf{\Gamma} \supset \mathbf{R}$ by viewing $\mathbf{R}$ as the set of constant polynomials.

2a: Nil-poly Thm. *In* $\mathbf{\Gamma} := \mathbf{R}[\![\mathsf{z}]\!]$, *a polynomial*

†: $\alpha := A_0 + A_1\mathsf{z} + \ldots + A_{S-1}\mathsf{z}^{S-1} + A_S\mathsf{z}^S$

$[S \in \mathbb{N}]$ *is* $\mathbf{\Gamma}$*-nilpotent IFF each* A_j *is* $\mathbf{R}$*-nilpotent.* ♢

Proof of (⇐). Each term $A_j\mathsf{z}^j$ is $\mathbf{\Gamma}$-nilpotent, since $\boldsymbol{\mathcal{N}}_{\mathbf{\Gamma}}$ is an ideal. Hence RhS(2a†) is in $\boldsymbol{\mathcal{N}}_{\mathbf{\Gamma}}$. ♦

Proof of (⇒). We now induct on S.

With $\mathcal{K} := \text{NilDeg}(\alpha)$, the high-order term of $\alpha^{\mathcal{K}}$ is $[A_S]^{\mathcal{K}}\mathsf{z}^{S\mathcal{K}}$, which must be zero. But $\mathsf{z}^{S\mathcal{K}}$ is not a zero-divisor, so $[A_S]^{\mathcal{K}}$ is zero, whence $\boxed{A_S \in \boldsymbol{\mathcal{N}}_{\mathbf{R}}}$.

Consequently, $\beta := A_S\mathsf{z}^S$ is nilpotent in $\mathbf{\Gamma}$. But $\boldsymbol{\mathcal{N}}_{\mathbf{\Gamma}}$ is an ideal, hence difference

$$\alpha - \beta \overset{\text{note}}{=\!=} A_0 + A_1\mathsf{z} + \ldots + A_{S-1}\mathsf{z}^{S-1}$$

is nilpotent. By induction, then, each coefficient $A_0, \ldots, A_{S-1}$ in nilpotent in $\mathbf{R}$. ♦

2b: Unit-poly Thm. *Consider elts* $u, A_1, \ldots, A_S \in \mathbf{R}$. *Then*

†: $\alpha := u + A_1\mathsf{z} + \ldots + A_{S-1}\mathsf{z}^{S-1} + A_S\mathsf{z}^S$

is a unit in $\mathbf{\Gamma} := \mathbf{R}[\![\mathsf{z}]\!]$ *IFF element* u *is an* $\mathbf{R}$*-unit and* $A_1, \ldots, A_S$ *are each* $\mathbf{R}$*-nilpotent.* ♢

Pf of (⇐). Elt $\gamma := A_1\mathsf{z} + \ldots + A_S\mathsf{z}^S$ is $\mathbf{\Gamma}$-nilpotent, so $u + \gamma$ is a unit, courtesy (1.4) ♦

Pf of (⇒) [web]. FTSOC, suppose (2b†) is a counterexample of minimum degree $S \geqslant 1$. ISTShow

∗: $$A_S \overset{?}{\in} \boldsymbol{\mathcal{N}}_{\mathbf{R}}\,.$$

For if so, then $\alpha - A_S\mathsf{z}^S$ is a unit, by (1.4), hence would be a counterexample of degree$<S$.

To establish this (2b∗), write unit $\beta := \alpha^{-1}$ as

‡: $\beta := B_0 + B_1\mathsf{z} + \ldots + B_T\mathsf{z}^T$ [with $B_T \neq 0$]

For $c \in [0\,..\,S{+}T]$, let $\overline{c}$ be the *coefficient* of z^c in $\alpha\beta$. Of course, the only non-zero $\overline{c}$ occurs at $c = 0$ [namely, $\overline{0} = 1$]. Since $S \geqslant 1$, then,

For $\boldsymbol{\ell} = 0, 1, \ldots, T$, *value* $\overline{S{+}T - \boldsymbol{\ell}}$ *is zero.*

We now inductively prove, for $n = 0, 1, \ldots, T$, that

$P(n)$: $$[A_S]^{n+1} \cdot B_{T-n} \;=\; 0\,.$$

Below, pair $\boldsymbol{(i,j)}$ ranges over all *ordered*-pairs of natnums that satisfy the conditions below the summation signs.

The base case is $0 = \overline{S{+}T} = A_S \cdot B_T$. Now fix $\boldsymbol{\ell} \in [1\,..\,T]$ for which $P(n)$ holds for each $n < \boldsymbol{\ell}$. Then

$$0 \;=\; \overline{S{+}T - \boldsymbol{\ell}} \;=\; \sum\nolimits_{i+j=\boldsymbol{\ell}} A_{S-i}B_{T-j}\,.$$

Multiplying by $[A_S]^{\boldsymbol{\ell}}$, and pulling out the $i{=}0$ term, gives

$$0 \;=\; [A_S]^{\boldsymbol{\ell}+1}B_{T-\boldsymbol{\ell}} + \sum_{\substack{i+j=\boldsymbol{\ell},\\ j<\boldsymbol{\ell}}} A_{S-i}[A_S]^{\boldsymbol{\ell}}B_{T-j}\,.$$

In the summation, our induction hypothesis says that each $[A_S]^{\boldsymbol{\ell}}B_{T-j}$ is zero, since $j < \boldsymbol{\ell}$. Hence $P(\boldsymbol{\ell})$.

Last step. We've established that $[A_S]^{T+1} \cdot B_0$ is zero. But $\alpha\beta = 1$, so $B_0 \overset{\text{note}}{=\!=} u^{-1}$ is a unit. Thus $[A_S]^{T+1}$ is zero. Hence (2b∗), as desired. ♦

Remark. An alternate proof of Unit-poly Thm, using ideals [and the Axiom of Choice] is below, in (7d). □

2c: McCoy's Thm. *In* $\mathbf{\Gamma} := \mathbf{R}[\![\mathsf{z}]\!]$, *an element*

†: $\alpha := A_0 + A_1\mathsf{z} + \ldots + A_{S-1}\mathsf{z}^{S-1} + A_S\mathsf{z}^S$

is a $\mathbf{\Gamma}$*–zero-divisor IFF there exists a non-zero* $w \in \mathbf{R}$ *such that* $\forall j$: $w{\cdot}A_j = 0$. [*IOWords, if* α *has a non-zero annihilator in* $\mathbf{\Gamma}$ *then* α *has a non-zero annihilator in* $\mathbf{R}$.] ♢

Proof [web]. Call a polynomial α "bad" if α is a zero-divisor, yet its only $\mathbf{R}$-annihilator is 0.

FTSOContradiction, consider a bad (2c†) and fix a non-Zip α-annihilator

‡: $\beta := B_0 + B_1\mathsf{z} + \ldots + B_T\mathsf{z}^T$ [with $B_T \neq 0$]

of *minimum degree*. Necessarily $T \geqslant 1$, since α is bad.

Could *every* $s \in [0\,..\,S]$, have $A_s\beta = 0$, forcing its high-order coeff A_sB_T to be zero? No, for this would imply that $\alpha B_T = 0$, showing α to be good.

Consequently, there is a *largest* index, $\boldsymbol{\sigma} \in [0\,..\,S]$, such that $\boxed{A_{\boldsymbol{\sigma}}\beta \neq 0}$. This gives us

$$[A_{\boldsymbol{\sigma}+1}\mathsf{z}^{\boldsymbol{\sigma}+1} + \ldots + A_S\mathsf{z}^S] \cdot \beta \;=\; 0\,. \quad \text{Thus,}$$
$$0 \overset{\text{recall}}{=\!=} \alpha\beta \;=\; [A_0 + A_1\mathsf{z} + \ldots + A_{\boldsymbol{\sigma}}\mathsf{z}^{\boldsymbol{\sigma}}] \cdot \beta\,,$$

which implies $A_{\boldsymbol{\sigma}}B_T = 0$. This last gives us that

$$\mathrm{Deg}(A_{\boldsymbol{\sigma}}\beta) \;<\; \mathrm{Deg}(\beta)\,.$$

But $0 = A_{\boldsymbol{\sigma}} \cdot \alpha\beta = \alpha \cdot [A_{\boldsymbol{\sigma}}\beta]$, and $A_{\boldsymbol{\sigma}}\beta \neq \text{Zip}$. So $\beta' := A_{\boldsymbol{\sigma}}\beta$ contradicts the minimalness of the degree of β. ♦

Properties of ideals

In commutative ring $\boldsymbol{\Gamma}$, recall that an ***ideal*** $\boldsymbol{\mathcal{I}} \subset \boldsymbol{\Gamma}$ is an additive-subgroup st. $\forall x \in \boldsymbol{\Gamma}$, necessarily $x\boldsymbol{\mathcal{I}} \subset \boldsymbol{\mathcal{I}}$. A ***proper*** ideal $\boldsymbol{\mathcal{I}}$ has $\boldsymbol{\mathcal{I}} \subsetneqq \boldsymbol{\Gamma}$. Evidently,

$$[\boldsymbol{\mathcal{I}} \not\ni 1] \;\; \text{IFF} \;\; [\boldsymbol{\mathcal{I}} \text{ is a proper ideal}]\,.$$

Use $\textsc{Ideal}_{\boldsymbol{\Gamma}}$ for the *set* of all ideals, and

3a: $$\textsc{Proper}_{\boldsymbol{\Gamma}} \;:=\; \textsc{Ideal}_{\boldsymbol{\Gamma}} \smallsetminus \{\boldsymbol{\Gamma}\}$$

for the set of *proper* ideals.

Given an arbitrary (possibly infinite) family $\mathcal{C}$ of ideals:

3b: *The intersection* $\bigcap(\mathcal{C})$ *is an ideal.*

Given a subset $S \subset \boldsymbol{\Gamma}$, there is a *unique smallest ideal* that includes S. Write it as

3c: $\langle\!\langle S \rangle\!\rangle = \langle\!\langle S \rangle\!\rangle_{\boldsymbol{\Gamma}} := \bigcap(\mathcal{C})$, *where* $\mathcal{C}$ *is the set of* $\boldsymbol{\Gamma}$*-ideals* $\boldsymbol{\mathcal{I}}$ *with* $\boldsymbol{\mathcal{I}} \supset S$.

Extend the notation so that $\langle\!\langle S_1, \ldots, S_N \rangle\!\rangle$ means $\langle\!\langle \bigcup_{j=1}^N S_j \rangle\!\rangle$. Extend further in that, for $\alpha \in \boldsymbol{\Gamma}$ and $S \subset \boldsymbol{\Gamma}$, have $\langle\!\langle \alpha, S \rangle\!\rangle$ mean $\langle\!\langle \{\alpha\}, S \rangle\!\rangle$.

3d: *Remark.* Every ideal $\boldsymbol{\mathcal{I}}$ satisfies that $\{0\} \subset \boldsymbol{\mathcal{I}} \subset \boldsymbol{\Gamma}$. The set of ideals, $\big(\textsc{Ideal}_{\boldsymbol{\Gamma}}, \subset\big)$, is a *complete lattice*, where the **meet** operation is *intersection*, and the **join** operation is $\langle\!\langle \cdot \rangle\!\rangle$. □

A subset $\mathcal{C} \subset \textsc{Ideal}_{\boldsymbol{\Gamma}}$ is a ***chain***, if $\mathcal{C}$ is totally-ordered by inclusion. Easily:

3e: *The union* $\bigcup(\mathcal{C})$ *of a chain-of-ideals, is itself an ideal.*

Operations on ideals. The ***sum*** of two ideals,

4a: $$\boldsymbol{\mathcal{A}} + \boldsymbol{\mathcal{B}} \;:=\; \{\alpha + \beta \mid \alpha \in \boldsymbol{\mathcal{A}} \text{ and } \beta \in \boldsymbol{\mathcal{B}}\}$$

is simply their set-theoretic sum, which is an ideal. Their ***product*** is

4b: $$\boldsymbol{\mathcal{A}\mathcal{B}} \;:=\; \left\{ \sum_{j=1}^{N} \alpha_j\beta_j \;\middle|\; \begin{array}{l} N \in \mathbb{N} \text{ with } \alpha_1, \ldots, \alpha_N \in \boldsymbol{\mathcal{A}} \\ \text{and } \beta_1, \ldots, \beta_N \in \boldsymbol{\mathcal{B}} \end{array} \right\}$$

Recall that the "***radical*** of ideal $\boldsymbol{\mathcal{I}}$" is

4c: $$\sqrt{\boldsymbol{\mathcal{I}}} \;:=\; \left\{ \alpha \in \boldsymbol{\Gamma} \;\middle|\; \exists \mathcal{K} \in \mathbb{Z}_+ \text{ with } \alpha^{\mathcal{K}} \in \boldsymbol{\mathcal{I}} \right\}.$$

and is itself [Lemma (1.2)] an ideal.

4d: *Defn.* Evidently, $\sqrt{\;}$ is *idempotent*; $\sqrt{\sqrt{\boldsymbol{\mathcal{I}}}} = \boldsymbol{\mathcal{I}}$. An ideal $\boldsymbol{\mathcal{I}}$ "is radical" if $\boldsymbol{\mathcal{I}} = \sqrt{\boldsymbol{\mathcal{I}}}$. □

4e: Lemma. *Suppose* $\mathcal{C}$ *is a collection of radical ideals. Then* $\boldsymbol{\mathcal{I}} := \bigcap(\mathcal{C})$ *is a radical ideal.*

Moreover, if $\mathcal{C}$ *is a chain, then* $\boldsymbol{\mathcal{U}} := \bigcup(\mathcal{C})$ *is a radical ideal.* ♢

Pf. Automatically $\boldsymbol{\mathcal{I}}$ is an ideal. Consider an $\alpha \in \boldsymbol{\Gamma}$ and posint $\mathcal{K}$ with $\alpha^{\mathcal{K}} \in \boldsymbol{\mathcal{I}}$. For *each* $\boldsymbol{\mathcal{A}} \in \mathcal{C}$, then, $\alpha^{\mathcal{K}} \in \boldsymbol{\mathcal{A}}$, since $\boldsymbol{\mathcal{I}} \subset \boldsymbol{\mathcal{A}}$. But $\boldsymbol{\mathcal{A}}$ is radical, so $\boldsymbol{\mathcal{A}} \ni \alpha$. Hence $\boldsymbol{\mathcal{I}} \ni \alpha$.

When $\mathcal{C}$ is a chain, then $\boldsymbol{\mathcal{U}}$ is an ideal. For an α with $\alpha^{\mathcal{K}} \in \boldsymbol{\mathcal{U}}$, there *exists* $\boldsymbol{\mathcal{A}} \in \mathcal{C}$ with $\alpha^{\mathcal{K}} \in \boldsymbol{\mathcal{A}}$. Hence $\boldsymbol{\mathcal{A}} \ni \alpha$, whence $\boldsymbol{\mathcal{U}} \ni \alpha$. ♦

Types of ideals

Henceforth, we assume the Axiom of Choice.

5a: *Partially-ordered Sets.* Here, symbols ω,α,β denote elements of poset $(\mathcal{P},\preccurlyeq)$. A ***maximal element*** ω has $\forall \omega' \in \mathcal{P}$: *If* $\omega' \succcurlyeq \omega$, *then* $\omega' = \omega$.

An ***upper-bound*** for a subet $S \subset \mathcal{P}$, is a $\beta \in \mathcal{P}$ st. $\alpha \preccurlyeq \beta$ for every $\alpha \in S$.

A ***chain*** is a subset $\mathcal{C} \subset \mathcal{P}$ that is totally-ordered under $\preccurlyeq$. □

5b: Zorn's Lemma. *In poset* $(\mathcal{P},\preccurlyeq)$, *suppose every chain admits an upper-bound.* [*The empty set is a chain, so this forces* $\mathcal{P} \neq \varnothing$.] *Then* $\mathcal{P}$ *has a maximal element.* ◊

Maximal ideals. Ideal $\mathcal{M}$ is a ***maximal ideal*** [more precisely, a ***maximal-proper ideal***] if $\mathcal{M}$ is a maximal element of poset $(\text{PROPER}_{\mathbf{\Gamma}}, \subset)$ of *proper* ideals of $\mathbf{\Gamma}$, ordered by inclusion. The std term is just "*maximal*", but we will use "***maxproper***" for clarity.

6a: *Defn.* For a subset $S \subset \mathbf{\Gamma}$, let $\text{AVOID}_S = \text{AVOID}_{S,\mathbf{\Gamma}}$ comprise those $\mathbf{\Gamma}$-ideals that are disjoint from S. For example, $\text{AVOID}_{\{1\},\mathbf{\Gamma}}$ is $\text{PROPER}_{\mathbf{\Gamma}}$. □

6b: Max-ideal Lemma. *For each* $S \subset \mathbf{\Gamma}$ *with* $S \not\ni 0$, *the poset* $(\text{AVOID}_S, \subset)$ *has a maximal element.* ◊

Pf. Since $0 \notin S$, our AVOID_S is non-empty, as it owns the zero-ideal. A chain $\mathcal{C} \subset \text{AVOID}_S$ engenders its union $\mathcal{U} := \bigcup(\mathcal{C})$, which an ideal that avoids S. So $\mathcal{U} \in \text{AVOID}_S$ is an upper-bound for $\mathcal{C}$. Zorn's guarantees the existence of a maximal element in AVOID_S. ♦

6c: Corollary. *Every ring admits a maxproper ideal.*
Proof. Apply (6b) with $S := \{1\}$. ◊

Prime ideals. Ideal $\mathcal{P}$ is ***prime*** if $\mathcal{P}$ is *proper* and:

> *For all* $x,y \in \mathbf{\Gamma}$, *if* $xy \in \mathcal{P}$, *then either* $x \in \mathcal{P}$ *or* $y \in \mathcal{P}$.

[So ideal $\{0\}$ is prime IFF $\mathbf{\Gamma}$ is an integral domain.]

7a: Lemma. *Each max-proper ideal* $\mathcal{M}$ *is prime. Each prime ideal* $\mathcal{P}$ *is radical.* ◊

Pf [*max* ⇒ *prime*]. By defn, $\mathcal{M}$ is proper. Consider $x_1, x_2 \notin \mathcal{M}$. Ideal $\mathcal{M} + x_j\mathbf{\Gamma}$ strictly extends $\mathcal{M}$, so $\mathcal{M} + x_j\mathbf{\Gamma} \overset{\text{must}}{=\!=} \mathbf{\Gamma}$. Thus $1 \in [x_j + \mathcal{M}]$. Hence

$$*: \qquad 1 \in [x_1 + \mathcal{M}][x_2 + \mathcal{M}] \subset x_1x_2 + \mathcal{M}\,.$$

But assertion $x_1 \cdot x_2 \in \mathcal{M}$, implies that $1 \in \mathcal{M}$; a contradition. ♦

Pf [*prime* ⇒ *radical*]. Say exponent $\mathcal{K} \in \mathbb{Z}_+$ is "good" if

$$\forall x \in \mathbf{\Gamma}: \quad [x^{\mathcal{K}} \in \mathcal{P}] \implies [x \in \mathcal{P}]\,.$$

Certainly $\mathcal{K}$=1 is good. Fix a good $\mathcal{K}$ and an x such that $x^{\mathcal{K}+1} \in \mathcal{P}$. By primeness, either $x \in \mathcal{P}$, or else $x^{\mathcal{K}} \in \mathcal{P}$; but this latter forces $x \in \mathcal{P}$. Hence $\mathcal{K}$+1 is good. Induction shows that every posint is good, so $\mathcal{P}$ is radical. ♦

7b: Prime/Nilradical Thm. *Let* $\mathcal{I}$ *denote the intersection of all prime ideals of* $\mathbf{\Gamma}$. *Then* $\mathcal{I} = \mathcal{N}_{\mathbf{\Gamma}}$, *the nilradical of* $\mathbf{\Gamma}$. ◊

Pf of (⊃). Why is $\mathcal{I} \supset \mathcal{N}_{\mathbf{\Gamma}}$? The foregoing says that $\mathcal{I}$ is radical. But $\{0\} \subset \mathcal{I}$, so $\sqrt{\{0\}} \subset \sqrt{\mathcal{I}} = \mathcal{I}$. ♦

Pf of (⊂) [*web*]. To establish the reverse, $\mathcal{I} \subset \mathcal{N}_{\mathbf{\Gamma}}$, ISTo fix a non-nilpotent element, ν, and produce a prime ideal $\mathcal{P}$ which does *not* own ν.

To $S := \{1, \nu, \nu^2, \nu^3, \ldots\}$, applying the Max-ideal Lemma (6b), produces a maximal ideal $\mathcal{P} \in \text{AVOID}_S$.

Showing $\mathcal{P}$ ***prime.*** Fixing $x,y \in \mathbf{\Gamma} \setminus \{\mathcal{P}\}$, it suffices to show that $xy \notin \mathcal{P}$.

Observe that ideal $\mathcal{P} + x\mathbf{\Gamma}$ [i.e, the $\mathcal{P}+\langle\!\langle x \rangle\!\rangle$ ideal] is strictly larger than $\mathcal{P}$. By maximality of $\mathcal{P}$, then,

$$\nu^{\mathcal{K}} \in \mathcal{P} + x\mathbf{\Gamma}\,, \qquad \text{for some posint } \mathcal{K}.$$

Similarly, $\nu^{\mathcal{L}} \in \mathcal{P} + y\mathbf{\Gamma}$ for some posint $\mathcal{L}$. Consequently, $\nu^{\mathcal{K}+\mathcal{L}} \in \mathcal{P} + xy\mathbf{\Gamma}$. Hence xy can*not* be in $\mathcal{P}$, else $\mathcal{P}$ would own $\nu^{\mathcal{K}+\mathcal{L}}$. ♦

7c: Quotient-ring Lemma. *For an ideal* $\mathcal{I}$ *of* $\mathbf{\Gamma}$:

†: *Quotient ring* $\mathbf{\Gamma}/\mathcal{I}$ *is a integral-domain IFF* $\mathcal{I}$ *is a prime ideal.*

‡: *Quotient ring* $\mathbf{\Gamma}/\mathcal{I}$ *is a field IFF* $\mathcal{I}$ *is a maxproper ideal.* ◊

Proof of (†). Well, $[x+\boldsymbol{\mathcal{I}}][y+\boldsymbol{\mathcal{I}}] = 0+\boldsymbol{\mathcal{I}}$ implies $xy \in \boldsymbol{\mathcal{I}}$ which, by primeness, implies WLOGenerality that $x \in \boldsymbol{\mathcal{I}}$, i.e, that $x+\boldsymbol{\mathcal{I}} = 0+\boldsymbol{\mathcal{I}}$.

Conversely, $xy \in \boldsymbol{\mathcal{I}}$ implies $[x+\boldsymbol{\mathcal{I}}][y+\boldsymbol{\mathcal{I}}] = 0+\boldsymbol{\mathcal{I}}$. This implies, since $\boldsymbol{\Gamma}/\boldsymbol{\mathcal{I}}$ is a domain, that WLOGenerality $x+\boldsymbol{\mathcal{I}} = 0+\boldsymbol{\mathcal{I}}$, i.e, that $x \in \boldsymbol{\mathcal{I}}$. ♦

Proof of (‡). Unfinished: as of 6Jul2018 ♦

7d: *Remark.* As an application of quotient rings, here is an alternative proof characterizing the units in a polynomial ring $\mathbf{R}[\![\mathsf{z}]\!]$. □

Pf of (2b), *Unit-poly Thm* [*web*]. Fix $\boldsymbol{\mathcal{P}} \subset \mathbf{R}$, a prime ideal of $\mathbf{R}$. Let $\overline{\mathbf{R}} := \mathbf{R}/\boldsymbol{\mathcal{P}}$ be the quotient ring, where $x \mapsto \overline{x}$ is the ring-hom $\mathbf{R} \to \overline{\mathbf{R}}$. This extends to a ring-hom $\mathbf{R}[\![\mathsf{z}]\!] \to \overline{\mathbf{R}}[\![\mathsf{z}]\!]$ which sends our $\mathbf{R}[\![\mathsf{z}]\!]$-unit

†: $$\alpha = u + A_1\mathsf{z} + \ldots + A_S\mathsf{z}^S \quad \text{to}$$
$$\overline{\alpha} = \overline{u} + \overline{A_1}\mathsf{z} + \ldots + \overline{A_S}\mathsf{z}^S .$$

Since $\overline{\alpha}$ is an $\overline{\mathbf{R}}[\![\mathsf{z}]\!]$-unit, and $\overline{\mathbf{R}}$ is an integral domain, it follows that each of $\overline{A_1}, \ldots, \overline{A_S}$ is $\overline{0}$. I.e

∗: *Coefficients* $A_1, \ldots, A_S$ *all lie in* $\boldsymbol{\mathcal{P}}$.

But (∗) holds for *every* prime ideal in $\mathbf{R}$.. So these coefficients lie in the intersection of the prime idelals which, by (7b), is the nilradical of $\mathbf{R}$. ♦

§Ring Index; symbols listed first