

Ring Notes

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage <http://squash.1gainesville.com/>
3 October, 2018 (at 09:02)

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 $\alpha \bullet \beta$.

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 $(\Gamma, +, 0)$ is a commutative group.

R3: Triple $(\Gamma, \cdot, 1)$ 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 $\alpha, x, y \in \Gamma$.

^{♥1}What I’m calling a semigroup is usually called a *monoid*. The std defn of *semigroup* does not require an identity-elt.

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

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

An $\alpha \in \Gamma$ is a Γ -*unit* if $\exists \beta \neq 0$ st. $\alpha\beta = 1 = \beta\alpha$.
Use Units_{Γ} or $\text{Units}(\Gamma)$

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

An intDomain F in which every non-zero element is a unit, $\text{Units}(F) = F \setminus \{0\}$, is a *field*. I.e. F is a commRing such that triple $(F \setminus \{0\}, \cdot, 1)$ 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: $\text{Units}(\mathbb{G})$ is cyclic, generated by i . And $\text{Units}(\mathbb{Z}_{12})$ is not cyclic. For which N is $\Phi(N)$ cyclic?] \square

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 $\text{ZD}(\Gamma)$ is disjoint from $\text{Units}(\Gamma)$.

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 $\alpha \blacktriangleright \beta$ [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 $\alpha \notin \text{ZD}$, 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

$$*: \quad \alpha = xy = \alpha cy.$$

By defn, $\alpha \notin \text{ZD}$. 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 \neq Prime.

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

Proof. Suppose $\alpha \bullet xy$ and WLOG $\alpha \nmid x$. 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

$$1 = S\alpha + Tx. \quad \text{Hence}$$

$$*: \quad y = S\alpha y + Txy = Sy\alpha + Txy.$$

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 $t \geq 0$:

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

And for $t \leq 0$ define

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

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

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

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 $[-2, 2] \setminus \{0\}$. Cty of g then forces $g = \mathbf{0}$.]

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

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

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

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

The “*radical* of \mathcal{I} ” is

$$3.1: \quad \sqrt{\mathcal{I}} := \left\{ \alpha \in \Gamma \mid \exists \mathcal{K} \in \mathbb{Z}_+ \text{ with } \alpha^{\mathcal{K}} \in \mathcal{I} \right\}.$$

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

3.2: **Lemma.** *The radical $\sqrt{\mathcal{I}}$ is itself an ideal.* \diamond

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

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

coefficient-times- $\alpha^k \beta^\ell$ terms,

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

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

Nilpotent elements. Element $\nu \in \Gamma$ 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 $\text{NilDeg}(\nu)$; remark that ν is a zero-divisor, since $\nu^{\mathcal{K}-1} \neq 0$, yet $0 = \nu^{\mathcal{K}-1} \cdot \nu$.

The set \mathcal{N}_{Γ} of nilpotent elements is called the “*nil-radical* of Γ ”. Evidently:

3.3: *The nilradical, $\mathcal{N}_{\Gamma} \stackrel{\text{note}}{=} \sqrt{\{0\}}$, is an ideal.*

3.4: **Lemma.** *In Γ , consider a unit u and nilpotent ν . Then $u + \nu$ and $u - \nu$ are units.* \diamond

Proof. ISTShow $u - \nu$ a unit. Element $\delta := u^{-1}\nu$ is nilpotent, since \mathcal{N}_{Γ} 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

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

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

Polynomial rings

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

4a: **Nil-poly Thm.** *In $\Gamma := \mathbf{R}[\mathbf{z}]$, a polynomial*

$$\dagger: \quad \alpha := A_0 + A_1 \mathbf{z} + \dots + A_{S-1} \mathbf{z}^{S-1} + A_S \mathbf{z}^S$$

[$S \in \mathbb{N}$] is Γ -nilpotent IFF each A_j is \mathbf{R} -nilpotent. \diamond

Proof of (\Leftarrow). Each term $A_j \mathbf{z}^j$ is Γ -nilpotent, since \mathcal{N}_{Γ} is an ideal. Hence $\text{Rhs}(4a\dagger)$ is in \mathcal{N}_{Γ} . \blacklozenge

Proof of (\Rightarrow). We now induct on S .

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

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

$$\alpha - \beta \stackrel{\text{note}}{=} A_0 + A_1 \mathbf{z} + \dots + A_{S-1} \mathbf{z}^{S-1}$$

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

4b: **Unit-poly Thm.** *Consider elts $u, A_1, \dots, A_S \in \mathbf{R}$. Then*

$$\dagger: \quad \alpha := u + A_1 \mathbf{z} + \dots + A_{S-1} \mathbf{z}^{S-1} + A_S \mathbf{z}^S$$

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

Pf of (\Leftarrow). Elt $\gamma := A_1 \mathbf{z} + \dots + A_S \mathbf{z}^S$ is Γ -nilpotent, so $u + \gamma$ is a unit, courtesy (3.4) \blacklozenge

Pf of (\Rightarrow) [web]. FTSOC, suppose (4b\dagger) is a counterexample of minimum degree $S \geq 1$. ISTShow

$$*: \quad A_S \stackrel{?}{\in} \mathcal{N}_{\mathbf{R}}.$$

For if so, then $\alpha - A_S \mathbf{z}^S$ is a unit, by (3.4), hence would be a counterexample of degree $< S$.

To establish this (4b*), write unit $\beta := \alpha^{-1}$ as

$$\ddagger: \quad \beta := B_0 + B_1 \mathbf{z} + \dots + B_T \mathbf{z}^T \quad [\text{with } B_T \neq 0]$$

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

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

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

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

Below, pair (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 $\ell \in [1 .. T]$ for which $P(n)$ holds for each $n < \ell$. Then

$$0 = \overline{S+T-\ell} = \sum_{i+j=\ell} A_{S-i} B_{T-j}.$$

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

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

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

Last step. We've established that $[A_S]^{T+1} \cdot B_0$ is zero. But $\alpha\beta = 1$, so $B_0 \stackrel{\text{note}}{=} u^{-1}$ is a unit. Thus $[A_S]^{T+1}$ is zero. Hence (4b*), as desired. \blacklozenge

Remark. An alternate proof of Unit-poly Thm, using ideals [and the Axiom of Choice] is below, in (9d). \square

4c: McCoy's Thm. In $\mathbf{\Gamma} := \mathbf{R}[\![z]\!]$, an element

$$\dagger: \quad \alpha := A_0 + A_1 z + \dots + A_{S-1} z^{S-1} + A_S z^S$$

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} .] \blacklozenge

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 (4c†) and fix a non-Zip α -annihilator

$$\ddagger: \quad \beta := B_0 + B_1 z + \dots + B_T z^T \quad [\text{with } B_T \neq 0]$$

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

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

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

$$[A_{\sigma+1} z^{\sigma+1} + \dots + A_S z^S] \cdot \beta = 0. \quad \text{Thus,}$$

$$0 \stackrel{\text{recall}}{=} \alpha \beta = [A_0 + A_1 z + \dots + A_\sigma z^\sigma] \cdot \beta,$$

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

$$\text{Deg}(A_\sigma \beta) < \text{Deg}(\beta).$$

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

Properties of ideals

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

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

Use $\text{IDEAL}_\mathbf{\Gamma}$ for the set of all ideals, and

$$5a: \quad \text{PROPER}_\mathbf{\Gamma} := \text{IDEAL}_\mathbf{\Gamma} \setminus \{\mathbf{\Gamma}\}$$

for the set of proper ideals.

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

$$5b: \quad \text{The intersection } \bigcap(\mathcal{C}) \text{ is an ideal.}$$

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

$$5c: \quad \langle\langle S \rangle\rangle = \langle\langle S \rangle\rangle_\mathbf{\Gamma} := \bigcap(\mathcal{C}), \text{ where } \mathcal{C} \text{ is the set of } \mathbf{\Gamma}\text{-ideals } \mathcal{I} \text{ with } \mathcal{I} \supset S.$$

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

5d: *Remark.* Every ideal \mathcal{I} satisfies that $\{0\} \subset \mathcal{I} \subset \Gamma$. The set of ideals, $(\text{IDEAL}_\Gamma, \subset)$, is a *complete lattice*, where the **meet** operation is *intersection*, and the **join** operation is $\langle\langle \cdot \rangle\rangle$. \square

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

5e: The union $\bigcup(\mathcal{C})$ of a chain-of-ideals, is itself an ideal.

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

$$6a: \mathcal{A} + \mathcal{B} := \{\alpha + \beta \mid \alpha \in \mathcal{A} \text{ and } \beta \in \mathcal{B}\}$$

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

$$6b: \mathcal{A}\mathcal{B} := \left\{ \sum_{j=1}^N \alpha_j \beta_j \mid \begin{array}{l} N \in \mathbb{N} \text{ with } \alpha_1, \dots, \alpha_N \in \mathcal{A} \\ \text{and } \beta_1, \dots, \beta_N \in \mathcal{B} \end{array} \right\}$$

Recall that the “**radical** of ideal \mathcal{I} ” is

$$6c: \sqrt{\mathcal{I}} := \{\alpha \in \Gamma \mid \exists \mathcal{K} \in \mathbb{Z}_+ \text{ with } \alpha^{\mathcal{K}} \in \mathcal{I}\}.$$

and is itself [Lemma (3.2)] an ideal.

6d: *Defn.* Evidently, $\sqrt{}$ is *idempotent*; $\sqrt{\sqrt{\mathcal{I}}} = \mathcal{I}$. An ideal \mathcal{I} “is radical” if $\mathcal{I} = \sqrt{\mathcal{I}}$. \square

6e: **Lemma.** Suppose \mathcal{C} is a collection of radical ideals. Then $\mathcal{I} := \bigcap(\mathcal{C})$ is a radical ideal.

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

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

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

Types of ideals

Henceforth, we assume the Axiom of Choice.

7a: *Partially-ordered Sets.* Here, symbols ω, α, β denote elements of poset (\mathcal{P}, \preceq) . A **maximal element** ω has $\forall \omega' \in \mathcal{P}$: If $\omega' \succ \omega$, then $\omega' = \omega$.

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

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

7b: **Zorn’s Lemma.** In poset (\mathcal{P}, \preceq) , suppose every chain admits an upper-bound. [The empty set is a chain, so this forces $\mathcal{P} \neq \emptyset$.] Then \mathcal{P} has a maximal element. \diamond

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

8a: *Defn.* For a subset $S \subset \Gamma$, let $\text{AVOID}_S = \text{AVOID}_{S, \Gamma}$ comprise those Γ -ideals that are disjoint from S . For example, $\text{AVOID}_{\{1\}, \Gamma}$ is PROPER_Γ . \square

8b: **Max-ideal Lemma.** For each $S \subset \Gamma$ with $S \not\ni 0$, the poset $(\text{AVOID}_S, \subset)$ has a maximal element. \diamond

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 . \diamond

8c: **Corollary.** Every ring admits a maxproper ideal. *Proof.* Apply (8b) with $S := \{1\}$. \diamond

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

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

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

9a: **Lemma.** Each max-proper ideal \mathcal{M} is prime. Each prime ideal \mathcal{P} is radical. \diamond

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

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

But assertion $x_1x_2 \in \mathcal{M}$, implies that $1 \in \mathcal{M}$; a contradiction. \blacklozenge

Pf [prime \Rightarrow radical]. Say exponent $\mathcal{K} \in \mathbb{Z}_+$ is “good” if

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

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. \blacklozenge

9b: Prime/Nilradical Thm. *Let \mathcal{I} denote the intersection of all prime ideals of Γ . Then $\mathcal{I} = \mathcal{N}_\Gamma$, the nilradical of Γ .* \blacklozenge

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

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

To $S := \{1, \nu, \nu^2, \nu^3, \dots\}$, applying the Max-ideal Lemma (8b), produces a maximal ideal $\mathcal{P} \in \text{AVOID}_S$.

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

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

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

Similarly, $\nu^{\mathcal{L}} \in \mathcal{P} + y\Gamma$ for some posint \mathcal{L} . Consequently, $\nu^{\mathcal{K}+\mathcal{L}} \in \mathcal{P} + xy\Gamma$. Hence xy cannot be in \mathcal{P} , else \mathcal{P} would own $\nu^{\mathcal{K}+\mathcal{L}}$. \blacklozenge

9c: Quotient-ring Lemma. *For an ideal \mathcal{I} of Γ :*

- \dagger : *Quotient ring Γ/\mathcal{I} is a integral-domain IFF \mathcal{I} is a prime ideal.*
- \ddagger : *Quotient ring Γ/\mathcal{I} is a field IFF \mathcal{I} is a maxproper ideal.* \blacklozenge

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

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

Proof of (\ddagger). *Unfinished: as of 30Oct2018* \blacklozenge

9d: Remark. As an application of quotient rings, here is an alternative proof characterizing the units in a polynomial ring $\mathbf{R}[[z]]$. \square

Pf of (4b), Unit-poly Thm [web]. Fix $\mathcal{P} \subset \mathbf{R}$, a prime ideal of \mathbf{R} . Let $\overline{\mathbf{R}} := \mathbf{R}/\mathcal{P}$ be the quotient ring, where $x \mapsto \overline{x}$ is the ring-hom $\mathbf{R} \rightarrow \overline{\mathbf{R}}$. This extends to a ring-hom $\mathbf{R}[[z]] \rightarrow \overline{\mathbf{R}}[[z]]$ which sends our $\mathbf{R}[[z]]$ -unit

$$\dagger: \quad \begin{aligned} \alpha &= u + A_1z + \dots + A_Sz^S & \text{to} \\ \overline{\alpha} &= \overline{u} + \overline{A_1}z + \dots + \overline{A_S}z^S. \end{aligned}$$

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

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

But ($*$) holds for *every* prime ideal in \mathbf{R} . So these coefficients lie in the intersection of the prime idelals which, by (9b), is the nilradical of \mathbf{R} . \blacklozenge

§Ring Index; symbols listed first

- $\sqrt{\mathcal{I}}$, 3
- $\Phi_N, \Phi(N), \varphi(N)$, 1
- \mathcal{N}_Γ , 3
- ZD_Γ or $\text{ZD}(\Gamma)$, 1
- annihilator, 1
- associates, 2
- associative, 1

- chain, 5
- commutative, 1

- distributes-over, 1

- field, 1

- Gaussian integers, 1
- group, 1

- ideal, 3, 4
 - zero-ideal, 3
 - maximal, *see* maxproper
 - maxproper, 5
 - prime, 5
 - proper, 4
 - radical, 5
- ideal, operations
 - product, 5
 - radical, 5
 - sum, 5
- identity element, 1
- integral domain, 1
- inverse element, 1
- irreducible element, 2

- Max-ideal lemma, 5
- maximal element, 5
- McCoy's thm, 4
- monoid, 1

- Nil-poly thm, 3
- nilpotent, 3
 - NilDeg(ν), 3
 - nilradical, 3

- prime element, 2

- radical operator $\sqrt{\mathcal{I}}$, 3
- ring, 1
 - domain, 1

- semigroup[=monoid], 1

- Theorems
 - Max-ideal, 5
 - McCoy's, 4
 - Nil-poly, 3
 - Unit-poly, 3
 - Zorn's, 5

- unit, 1, 2
- Unit-poly thm, 3
- Units $_\Gamma$ or Units(Γ), 1
- upper-bound, 5

- ZD, *i.e.*: zero-divisor
- zero-divisor, 1, 2
- Zorn's lemma, 5