XIV Summer Workshop in Mathematics MAT/UnB

Formalizing Theorems with PVS

Section 3: Pen and paper proofs versus formal proofs

Thaynara Arielly de Lima (IME) UFG
Mauricio Ayala-Rincón (CIC-MAT) UnB

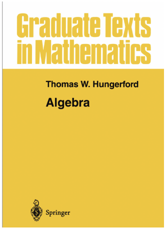
Funded by FAPDF DE grant 00193.0000.2144/2018-81, CNPq Research Grant 307672/2017-4

Jan 17 - 21 , 2021

Talk's Plan

1. Section 3
   - Formalizing a simple remark in Hungerford's abstract algebra textbook

Hungerford's remark



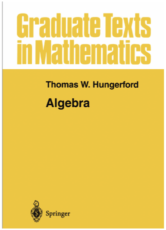
Definition 3.5. *An integral domain* R *is a* **unique factorization domain** *provided that:*

(i) *every nonzero nonunit element* a *of* R *can be written* $a = c_1c_2\cdots c_n$, *with* $c_1, \ldots, c_n$ *irreducible.*

(ii) *If* $a = c_1c_2\cdots c_n$ *and* $a = d_1d_2\cdots d_m$ (c_i, d_i *irreducible*), *then* $n = m$ *and for some permutation* σ *of* $\{1,2,\ldots,n\}$, c_i *and* $d_{\sigma(i)}$ *are associates for every* i.

REMARK. Every irreducible element in a unique factorization domain is necessarily prime by (ii). Consequently, irreducible and prime elements coincide by Theorem 3.4 (iii).

Hungerford's remark - Ring definition



Definition 1.1. *A* **ring** *is a nonempty set* R *together with two binary operations (usually denoted as addition* (+) *and multiplication) such that:*

(i) (R,+) *is an abelian group;*
(ii) (ab)c = a(bc) *for all* a,b,c ε R *(associative multiplication);*
(iii) a(b + c) = ab + ac *and* (a + b)c = ac + bc *(left and right distributive laws).*

If in addition:

(iv) ab = ba *for all* a,b ε R,

then R *is said to be a* **commutative ring.** *If* R *contains an element* 1_R *such that*
(v) $1_R a = a 1_R = a$ *for all* a ε R,

then R *is said to be a* **ring with identity.**

See the file `ring_def.pvs` in https://github.com/nasa/pvslib/tree/master/algebra

Hungerford's remark - Ring examples

$(\mathbb{Z}, +, \cdot, 0, 1)$

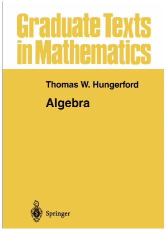
$(m\mathbb{Z} = \{m \cdot z; z \in \mathbb{Z}$ and m is a natural number $\}, +, \cdot, 0)$

$(\{f : \mathbb{R} \to \mathbb{R}\}, + : (f+g)(x) = f(x) + g(x), \cdot : (f \cdot g)(x) = f(x) \cdot g(x), 0, 1)$

$$\left(M_2(\mathbb{R}) = \left\{ \left(\begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right); a_{ij} \in \mathbb{R} \right\}, +_{:} M_2(\mathbb{R}), \cdot_{:} M_2(\mathbb{R}), \left(\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)\right)$$

$(\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}, + : \overline{a} + \overline{b} = \overline{a+b}, \cdot : \overline{a} \cdot \overline{b} = \overline{a \cdot b}, \overline{0})$

Hungerford's remark

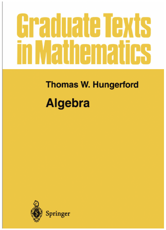


Definition 1.3. *A nonzero element* a *in a ring* R *is said to be a* **left** [*resp. right*] **zero divisor** *if there exists a nonzero* b ε R *such that* ab = 0 [*resp.* ba = 0]. *A* **zero divisor** *is an element of* R *which is both a left and a right zero divisor.*

See the file `ring_nz_closed_def.pvs` in

https://github.com/nasa/pvslib/tree/master/algebra

Hungerford's remark

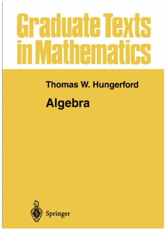


Definition 1.5. *A commutative ring* R *with identity* $1_R \neq 0$ *and no zero divisors is called an* **integral domain.** *A ring* D *with identity* $1_D \neq 0$ *in which every nonzero element is a unit is called a* **division ring.** *A* **field** *is a commutative division ring.*

See the file `integral_domain_with_one_def.pvs` in

https://github.com/nasa/pvslib/tree/master/algebra

Hungerford's remark



Definition 1.4. *An element* a *in a ring* R *with identity is said to be* **left** [*resp. right*] **invertible** *if there exists* $c \in R$ [*resp.* $b \in R$] *such that* $ca = 1_R$ [*resp.* $ab = 1_R$]. *The element* c [*resp.* b] *is called a* **left** [*resp. right*] **inverse** *of* a. *An element* $a \in R$ *that is both left and right invertible is said to be* **invertible** *or to be a* **unit.**

Definition 3.1. *A nonzero element* a *of a commutative ring* R *is said to* **divide** *an element* $b \in R$ (*notation:* $a \mid b$) *if there exists* $x \in R$ *such that* $ax = b$. *Elements* a,b *of* R *are said to be* **associates** *if* $a \mid b$ *and* $b \mid a$.

Definition 3.3. *Let* R *be a commutative ring with identity. An element* c *of* R *is* **irreducible** *provided that:*

(i) c *is a nonzero nonunit;*
(ii) $c = ab \implies$ a *or* b *is a unit.*

An element p *of* R *is* **prime** *provided that:*

(i) p *is a nonzero nonunit;*
(ii) $p \mid ab \implies p \mid a$ *or* $p \mid b$.

Hungerford's remark

- In $\mathbb{Z}$, the notions of prime and irreducible elements are equal.
- In $\mathbb{Z}_6$, 2 is a prime element; however 2 is not an irreducible element.

Hungerford's remark

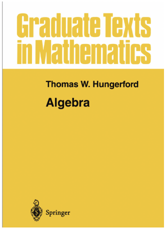
Every prime element in an integral domain R is an irreducible element.

If $p = ab$ then $p|a$ or $p|b$ since $p|p = ab$ and p is prime.

Consider that $p|a$. Thus $a = px$ and $p = ab = pxb$.

Consequently, $p - pxb = p(one - xb) = zero$. Thus, $xb = one$ and b is an unit.

Hungerford's remark



Definition 3.5. *An integral domain* R *is a* **unique factorization domain** *provided that:*

(i) *every nonzero nonunit element* a *of* R *can be written* $a = c_1c_2\cdots c_n$, *with* $c_1, \ldots, c_n$ *irreducible.*

(ii) *If* $a = c_1c_2\cdots c_n$ *and* $a = d_1d_2\cdots d_m$ (c_i, d_i *irreducible*), *then* $n = m$ *and for some permutation* σ *of* $\{1,2,\ldots,n\}$, c_i *and* $d_{\sigma(i)}$ *are associates for every* i.

REMARK. Every irreducible element in a unique factorization domain is necessarily prime by (ii). Consequently, irreducible and prime elements coincide by Theorem 3.4 (iii).