



XXIX Semana do IME/UFG e VI Seminário de Pesquisa e Pós-Graduação do IME/UFG

Formalização de Teoremas em Assistentes de Prova

Section 3: Provas em papel e lápis versus provas formais

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

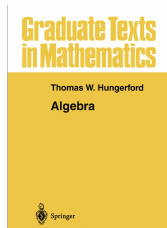
Oct 6 -8 , 2021

Talk's Plan

1 Section 3

- Formalizing a simple remark in Hungerford's abstract algebra textbook

Hungerford's remark

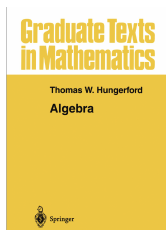


Definition 3.5. *An integral domain R is a unique factorization domain provided that:*

- (i) *every nonzero nonunit element a of R can be written $a = c_1 c_2 \cdots c_n$, with c_1, \dots, c_n irreducible.*
- (ii) *If $a = c_1 c_2 \cdots c_n$ and $a = d_1 d_2 \cdots d_m$ (c_i, d_i irreducible), then $n = m$ and for some permutation σ of $\{1, 2, \dots, n\}$, 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 $a, b, c \in R$ (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 $a, b \in R$,

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 $a \in R$,

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

See the file [ring_def.pvs](https://github.com/nasa/pvslib/tree/master/algebra) in <https://github.com/nasa/pvslib/tree/master/algebra>

Hungerford's remark - Ring examples

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

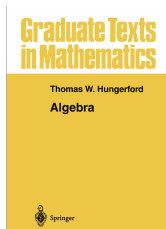
$$(m\mathbb{Z} = \{m \cdot z; z \in \mathbb{Z} \text{ and } m \text{ is a natural number}\}, +, \cdot, 0)$$

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

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

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

Hungerford's remark

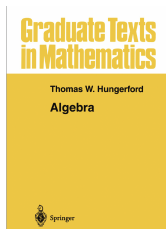


Definition 1.3. *A nonzero element a in a ring R is said to be a **left** [resp. **right**] **zero divisor** if there exists a nonzero $b \in R$ such that $ab = 0$ [resp. $ba = 0$]. A **zero divisor** is an element of R which is both a left and a right zero divisor.*

See the file `ring_nz_closed_def.pvs` in

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

Hungerford's remark

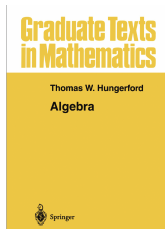


Definition 1.5. *A commutative ring R with identity $1_R \neq 0$ and no zero divisors is called an **integral domain**. A ring D with identity $1_D \neq 0$ in which every nonzero element is a unit is called a **division ring**. A **field** is a commutative division ring.*

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) $c = ab \Rightarrow a$ or b is a unit.

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

- (i) p is a nonzero nonunit;
- (ii) $p \mid ab \Rightarrow p \mid a$ 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

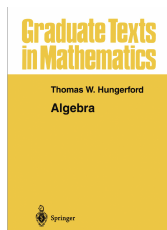
Every prime element in an integral domain R is an irreducible element.

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, $p - pxb = p(\text{one} - xb) = \text{zero}$. Thus, $xb = \text{one}$ 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 $a = c_1 c_2 \cdots c_n$, with c_1, \dots, c_n irreducible.*
- (ii) *If $a = c_1 c_2 \cdots c_n$ and $a = d_1 d_2 \cdots d_m$ (c_i, d_i irreducible), then $n = m$ and for some permutation σ of $\{1, 2, \dots, n\}$, 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).