XIV Summer Workshop in Mathematics MAT/UnB

19o Seminário Informal (+Formal!) do Grupo de Teoria da Computação da UnB

Formalizing Theorems with PVS

Section 3: Pen-and-paper proofs vs Formal proofs

Thaynara Arielly de Lima (IME)

Mauricio Ayala-Rincón (CIC-MAT)

Funded by FAPDF DE grants 00193.0000.2144/2018-81, 00193-00000229/2021-21, and CNPq Research Grants 307672/2017-4 and 313290/2021-0

Jan 17 - 21 , 2022

Talk's Plan

1. Summarizing the benefits of mechanical theorem proving
2. The general version of Chinese Remainder Theorem
3. A simple remark in Hungerford's textbook
    - Formalizing a simple remark in Hungerford's abstract algebra textbook

What are the benefits that could be obtained from mechanical theorem proving?

- To improve the capability to detect flaws, omissions, redundancies, and errors in pen-and-paper proofs.
- To increase the ability to provide precise and complete formulations of definitions, theorems, and proofs.
- To refine the precision grade to formulate feasible conjectures and consequently the capability to discover new results.
- To fix the required discipline and organization to compile and communicate reliable and reproducible mathematical knowledge.
- Moreover, and the most important, to provide a thoughtful and rigorous understanding of any mathematical theory.

Interesting opinions in: Jeremy Avigad *"The Mechanization of Mathematics"* - Notices of the AMS 2018

"But the mathematical literature is filled with errors, ranging from typographical errors, missing hypotheses, and overlooked cases to mistakes that invalidate a substantial result."

"The situation will only get worse as proofs get longer and more complex. In a 2008 opinion piece in the Notices, "Desperately seeking mathematical truth", Melvyn Nathanson lamented the difficulties in certifying mathematical results: "We mathematicians like to talk about the 'reliability' of our literature, but it is, in fact, unreliable." "

"Checking the details of a mathematical proof is far less enjoyable than exploring new concepts and ideas, but it is important nonetheless. Rigor is essential to mathematics, and even minor errors are a nuisance to those trying to read, reconstruct, and use mathematical results."

Chinese Remainder Theorem - The integer version

Consider $m_1, \ldots, m_r$ positive integers such that m_i and m_j are coprime for $i \neq j$ and $m = m_1 \ldots m_r$. Thus,

$$\mathbb{Z}/(m_1 \ldots m_r)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$$

In other notation

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$$

Chinese Remainder Theorem - The general version for Rings

Let R be a ring with identity and $A_1, A_2, \ldots, A_k$ ideals in R. If the condition $A_i + A_j = R$ holds for each $i, j \in \{1, \ldots, k\}$ with $i \neq j$, which is called comaximality, then

$$R/(A_1 \cap \ldots \cap A_k) \cong R/A_1 \times \ldots \times R/A_k$$

Step 1: Prove that

$$\begin{array}{rccc} \varphi: & R & \to & R/A_1 \times \ldots \times R/A_k \\ & r & \mapsto & (r + A_1, \ldots, r + A_k) \end{array}$$

is a ring homomorphism with kernel $A_1 \cap \ldots \cap A_k$;

Chinese Remainder Theorem - The general version for Rings

Step 2: Prove that

$$\begin{array}{rccc} \varphi: & R & \to & R/A_1 \times \ldots \times R/A_k \\ & r & \mapsto & (r + A_1, \ldots, r + A_k) \end{array}$$

is a surjective function;

Step 3: Conclude the result by the First Isomorphism for Rings.

Chinese Remainder Theorem - The general version for Rings

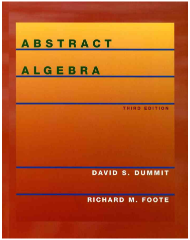
Theorem 17. *(Chinese Remainder Theorem)* Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \quad \text{defined by} \quad r \mapsto (r+A_1, r+A_2, \ldots, r+A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

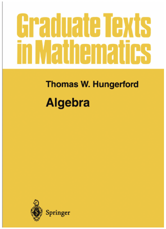
Sec. 7.6 The Chinese Remainder Theorem 265



Proof: We first prove this for $k = 2$; the general case will follow by induction. Let $A = A_1$ and $B = A_2$. Consider the map $\varphi : R \to R/A \times R/B$ defined by $\varphi(r) = (r \bmod A, r \bmod B)$, where mod A means the class in R/A containing r (that is, $r + A$). This map is a ring homomorphism because φ is just the natural projection of R into R/A and R/B for the two components. The kernel of φ consists of all the elements $r \in R$ that are in A and in B, i.e., $A \cap B$. To complete the proof in this case it remains to show that when A and B are comaximal, φ is surjective and $A \cap B = AB$. Since $A + B = R$, there are elements $x \in A$ and $y \in B$ such that $x + y = 1$. This equation shows that $\varphi(x) = (0, 1)$ and $\varphi(y) = (1, 0)$ since, for example, x is an element of A and $x = 1 - y \in 1 + B$. If now $(r_1 \bmod A, r_2 \bmod B)$ is an arbitrary element in $R/A \times R/B$, then the element $r_2 x + r_1 y$ maps to this element since

- In order to formalize that phi is a homomorphism, one must verify that for all $j \leq k$, and a, b in R, $(a+b)+A_j = (a+A_j)+(b+A_j)$ holds (`quotient_rings@add_charac`).
- It has an equivalent cost of the analysis for two ideals in a proof by induction, where $k=2$.
- In the induction step, the analysis given for two ideals cannot be repeated in a straightforward manner: one has to build structures such as an ideal A such that $(R/A_1 \times \ldots \times R/A_n) \simeq R/A$, to be able to apply the reasoning for two ideals to conclude that the map `phi` is a homomorphism from R to $R/A \times R/A_{n+1}$.

Hungerford's remark



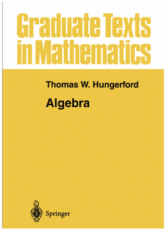
Definition 3.5. *An integral domain* R *is a* **unique factorization domain** *provided that:*

(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

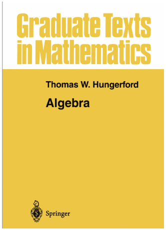


Definition 1.5. *A commutative ring* R *with identity* $1_R \neq 0$ *and no zero divisors is called an* **integral domain.** *A ring* D *with identity* $1_D \neq 0$ *in which every nonzero element is a unit is called a* **division ring.** *A* **field** *is a commutative division ring.*

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

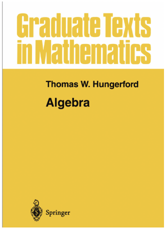
Every prime element in an integral domain R is an irreducible element.

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).