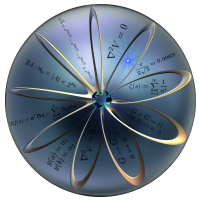

planetmath.org

Math for the people, by the people.

Chinese remainder theorem for rings, noncommutative case

Canonical name	ChineseRemainderTheoremForRingsNoncommutativeCase
Date of creation	2013-03-22 16:53:45
Last modified on	2013-03-22 16:53:45
Owner	polarbear (3475)
Last modified by	polarbear (3475)
Numerical id	16
Author	polarbear (3475)
Entry type	Theorem
Classification	msc 13A15
Classification	msc 11D79
Synonym	chinese remainder theorem

Theorem 1. *(**Chinese Remainder Theorem**) Let R be a ring and $I_1, I_2, ..., I_n$* `http://planetmath.org/Comaximal`*pairwise comaximal ideals such that $R = I_j + R^2$ for all j. The homomorphism:*

$$f : R \to R/I_1 \times R/I_2 \times ... \times R/I_n$$
$$f(a) = (a + I_1, a + I_2, ..., a + I_n)$$

is surjective and $ker f = I_1 \cap I_2 \cap \cdots \cap I_n$.

Proof. Clearly f is a homomorphism with kernel $I_1 \cap I_2 \cap \cdots \cap I_n$. It remains to show the surjectivity.
We have:

$$\begin{aligned} R = I_1 + R^2 &= I_1 + (I_1 + I_2)(I_1 + I_3) \\ &\subseteq I_1 + I_1^2 + I_1 I_3 + I_2 I_1 + I_2 I_3 \\ &\subseteq I_1 + (I_2 \cap I_3). \end{aligned}$$

Moreover,

$$\begin{aligned} R = I_1 + R^2 &= I_1 + (I_1 + I_2 \cap I_3)(I_1 + I_4) \\ &= I_1 + I_1 I_4 + (I_2 \cap I_3) I_1 + (I_2 \cap I_3) I_4 \\ &\subseteq I_1 + (I_2 \cap I_3 \cap I_4). \end{aligned}$$

Continuing, we obtain that $R = I_1 + \bigcap_{j \neq 1} I_j$. We show similarly that:

$$R = I_2 + \bigcap_{j \neq 2} I_j = I_3 + \bigcap_{j \neq 3} I_j = \cdots = I_n + \bigcap_{j \neq n} I_j.$$

Given elements $a_1, a_2, ..., a_n$, we can find $x_j \in I_j$ and $y_j \in \bigcap_{j \neq k} I_k$ such that $a_j = x_j + y_j$.
Take $a := \sum_{i=1}^{n} x_i = a_j \pmod{I_j}$.
Hence

$$f(a) = (a_1 + I_1, a_2 + I_2, ..., a_n + I_n),$$

and we conclude that f is surjective as required. □

Notes 1.The relation $R = I_j + R^2$ is satisfied when R is ring with unity. In that case $R^2 = R$.
2. The `http://planetmath.org/ChineseRemainderTheorem`Chinese Remainder Theorem case for integers is obtained from the above result. For this, take $R = \mathbb{Z}$ and $I_j = (p_j) = p_j\mathbb{Z}$. The fact that two solutions of the set of congruences must $x = x_0 \pmod{p_1...p_n}$ is a consequence of:

$$I_1 \cap I_2 \cap \cdots \cap I_n = (p_1) \cap (p_2) \cap \cdots \cap (p_n) = (p_1 p_2 ... p_n)\mathbb{Z}.$$