M3P8 LECTURE NOTES 4: THE CHINESE REMAINDER THEOREM

1. Products

Let R and S be rings. The *direct product* $R \times S$ is a ring whose elements are pairs (r, s) with $r \in R$, $s \in S$. The addition and multiplication are given componentwise:

$$(r, s) + (r', s') = (r + r', s + s')$$
$$(r, s)(r', s') = (rr', ss')$$

.

The product comes with two natural homomorphisms π_1, π_2 (projection onto the first and second factors) defined by:

$$\pi_1(r, s) = r : R \times S \to R$$

$$\pi_2(r, s) = s : R \times S \to S$$

and the following universal property:

Proposition 1.1. *Let T be any ring. For any pair $f : T \to R$, $g : T \to S$ of homomorphisms, there is a unique homomorphism $f \times g : T \to R \times S$ such that $\pi_1 \circ (f \times g) = f$ and $\pi_2 \circ (f \times g) = g$.*

Proof. The homomorphism $f \times g$ is defined by $(f \times g)(t) = (f(t), g(t))$; one checks easily that it is the unique map $T \to R \times S$ with the given property. $\square$

One can define multiple products $R_1 \times R_2 \times \cdots \times R_n$ inductively, by iterating the above process. More generally, if I is any index set, and for each $i \in I$ we have a ring R_i, we can define the product $\prod_i R_i$. An element r of this product is a choice, for each $i \in I$, of an element of R_i; we write such an element as $(r_i)_{i \in I}$. For each $j \in I$ we have a map $\pi_j : \prod_i R_i \to R_j$ given by $\pi_j((r_i)_{i \in I}) = r_j$.

Such a product satisfies a very similar universal property: for any collection $f_i : T \to R_i$ of maps for each $i \in I$, we get a unique map $\prod_i f_i : T \to \prod_i R_i$ such that $\pi_j \circ \prod_i f_i = f_j$.

2. The Chinese Remainder Theorem

Let R be a ring, and let $I_1, \ldots, I_n$ be a finite collection of ideals of R. For each j, we have the natural map $R \to R/I_j$, which is surjective with kernel I_j.

Consider the product map:

$$R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

It is easy to see that the kernel of this map is the intersection $I_1 \cap I_2 \cap \cdots \cap I_n$. Call this ideal J. We thus have an embedding:

$$R/J \hookrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

A natural question to ask is, what can we say about the image? In other words, given congruence classes mod I_1, I_2, etc., when is there a *single* element of R that lives in all those congruence classes simultaneously? Note that (because the above map is injective) if one such element exists, then there is a unique congruence class modulo J that satisfies all of the required congruences.

Of course, without further hypotheses we can't expect this map to be surjective (think about what happens when $I_1 = I_2$, for instance.) Nonetheless, we have:

Theorem 2.1. *Suppose that for each $i \neq j$, the sum $I_i + I_j$ is the unit ideal. Then the natural map:*

$$R/J \hookrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

is an isomorphism.

Proof. We have to prove it is surjective. It suffices to construct, for each i, an element e_i of R that is congruent to 1 modulo I_i and zero modulo I_j for $j \neq i$. (Suppose we have such an element. Then for any tuple $(r_1, \dots, r_n)$ of elements of r, the element $r_1 e_1 + \cdots + r_n e_n$ is congruent to r_i modulo I_i for all i.)

Given $i \neq j$, we know $I_i + I_j$ is the unit ideal; that is, we can write $1 = r + s$ with $r \in I_i$ and $s \in I_j$. Then s is congruent to 1 mod I_i and 0 mod I_j. Set $f_{ij} = s$. Then for any i we can take $e_i = \prod_{j \neq i} f_{ij}$, and e_i will be 1 mod I_i and zero modulo I_j for $j \neq i$. The result follows. $\square$

3. Examples

When $R = \mathbb{Z}$, then every ideal is principal, so we can write $I_i = \langle n_i \rangle$ for all i. The condition that $I_i + I_j$ is the unit ideal becomes the condition that the integers n_i are pairwise relatively prime. In this case the ideal J is generated by the product n of the n_i. Specializing, we find the version of the Chinese Remainder Theorem from elementary number theory:

Theorem 3.1. *If $\{n_i\}$ is a finite collection of pairwise relatively prime integers, and n is their product, then for any integers a_i, there is an integer a (unique up to congruence mod n) such that a is congruent to a_i mod n_i for all i.*

Now let K be a field and take $R = K[X]$. Then if $a_1, \dots, a_n$ are distinct elements of K, the ideals $I_i = \langle X - a_i \rangle$ are pairwise relatively prime. Moveover, for each i, I_i is the kernel of the evaluation map $K[X] \to K$ that takes X to a_i. We thus have an isomorphism of $K[X]/I_i$ with K that takes $P(X)$ to $P(a_i)$ for all polynomials P. We thus obtain:

Theorem 3.2. *For any* $c_1, \ldots, c_n \in K$*, There is a polnyomial* $P(X)$ *in* $K[X]$*, unique up to congruence modulo* $(x - a_1)(x - a_2)\ldots(x - a_n)$ *such that* $P(a_i) = c_i$ *for all* i*.*