Algebraic Theory I

Thomas Fleming

November 15, 2021

Contents

1 Chinese Remainder Theorem

Lecture 34: Chinese Remainder Theorem

Fri 12 Nov 2021 17:29

Theorem 1.1 (Classical Chinese Remainder Theorem)**.** If $m_1, \ldots, m_r$ are relatively prime integers, then for $a_1, \ldots, a_r$ we find an $x \in \mathbb{Z}$ so that $x \equiv a_i \mod m_i$ for each $1 \leq i \leq r$.

Theorem 1.2 (Generalized Chinese Remainder Theorem)**.** Let R be a commutative ring with $I_1, \ldots, I_n \subseteq R$ being ideals so that $I_i + I_j = R$ for all $i \neq j$. That is, the I_is are pairwise co-maximal. Then for any $x_1, \ldots, x_n \in R$ we find an $x \in R$ so that $x \equiv x_i \mod I_i$ for all $1 \leq i \leq n$.

Recall. $x \equiv x_i \mod I_i$ if $x - x_i \in I_i$.

Proof. If $n = 1$ this is trivial. Of course, $x = x$.
For the case $n = 2$ we have $I_1 + I_2 = R$, hence $1 \in R = I_1 + I_2$. Hence, $1 = a_1 + a_2$ with $a_1 \in I_1, a_2 \in I_2$. Then, let $x = x_1 a_1 + x_2 a_2$, and we see $a_1 + a_2 = 1$ but $a_1 \equiv 0 \mod I_1$ and likewise $a_2 \equiv 0 \mod I_2$, hence $a_1 \equiv 1 \mod I_2$ and $a_2 \equiv 1 \mod I_1$. Hence,

$$\begin{aligned}
x &= x_1 a_2 + x_2 a_1 \\
&\equiv x_1 a_2 \mod I_1 \\
&\equiv x_1 \mod I_1 \\
\text{and } x &\equiv x_2 a_1 \\
&\equiv x_2 \mod I_2.
\end{aligned}$$

Hence, the claim holds for $n = 2$. Now, we induce on n.
Let $n \geq 3$ and suppose the case $n - 1$ to be true. Then, we find Then, we see

$I_1 + I_i = R$ for all $i \geq 2$ by hypothesis. Hence, $1 = a_i + b_i$ with $a_i \in I_1$, $b_i \in I_i$. Then, we find

$$1 = \underbrace{1 \cdot \ldots \cdot 1}_{n \text{ times}} = \prod_{i=1}^{n} (a_i + b_i) \in \prod_{i=1}^{n} (I_1 + I_i) \subseteq I_1 + \prod_{i=2}^{n} I_i.$$

Moreover, we know $I_1 + \prod_{i=2}^{n} I_i$ to be an ideal as the product and sum of ideals are still ideals.
Then applying the case $n = 2$, we find a $y \in R$ so that $y_1 \equiv 1 \mod I_1$ and $y_1 \equiv 0 \mod \prod_{i=2}^{n} I_i$. Repeating for each $1 \leq i \leq n$ yields a $y_j \in R$ so that $y_j \equiv 1 \mod I_j$ and $y_j \equiv 0 \mod \prod_{1 \leq i \leq n; i \neq j} I_i$. Now, define $x = \prod_{i=1}^{n} x_i y_i$. We see $y_j \in I_i$ for all $i \neq j$, hence $y_j x_j \equiv 0 \mod I_i$ for all $i \neq j$. Hence $x \equiv x_i y_i \equiv x_i \mod I_i$. □

Note that in the preceding proof $\prod I_i$ denotes the ideal product as defined in the homework. In the next theorem we will use this symbol for the cartesian product, so ideal products will be written without product notation when the context is not necessarily clear.

Corollary 1 (Alternative Statement of the Chinese Remainder Theorem)**.** Let R be a commutative ring with $I_1, \ldots, I_n \subseteq R$ being pairwise comaximal distinct ideals of R. Then the map

$$\begin{aligned} f : R &\longrightarrow \prod_{i=1}^{n} R/I_i \\ x &\longmapsto (x \mod I_i)_{1 \leq i \leq n} \end{aligned}$$

is a surjective ring homomorphism with kernel $\ker(f) = \bigcap_1^n I_i$. Specifically,

$$R/\left(\bigcap_{i=1}^{n} I_i\right) \simeq \prod_{i=1}^{n} (R/I_i).$$

Proof. It is easily confirmed that f is a ring homomorphism with the prescribed kernel. Hence, the only claim that remains to be shown is the surjectivity. For f to be surjective, we need to take an arbitrary congruence system $\hat{x} = (x_1 \mod I_1, x_2 \mod I_2, \ldots, x_n \mod I_n)$ in the codomain of f and find a solution $x \in R$ so that $x \equiv x_i \mod I_i$ for all $1 \leq i \leq n$ (that is $f(x) = \hat{x}$). We see the generalized remainder theorem yields such an x, so f is surjective. □

2 Polynomial Rings

Lecture 35: Polynomials

Mon 15 Nov 2021 11:32

Definition 2.1 (Polynomial Ring)**.** Let R be a commutative ring and we define $R[X]$ to be the ring of polynomials in the variable x with coefficients from R defined as follows.
An element $f \in R[X]$ has the form

$$f = a_0 + a_1 x + \ldots + a_n x^n$$

for some $n \geq 0$ and each $a_i \in R$. This is a formal sum in the sense that two polynomials

$$f = a_0 + a_1 x + \ldots + a_n x^n$$
$$g = b_0 + b_1 x + \ldots b_m x^m$$

have $f = g$ if and only if $a_i = b_i$ for every i.
For the polynomial f, we call a_0 the **constant term** and a_n to be the **leading coefficient** and n to be the **degree**, denoted $\deg(f) = n$.
For the polynomial $f = 0$, we specifically define $\deg(f) = -1$. For all other constant polynomials g, we define $\deg(g) = 0$.

Remark. Occasionally, we will write $f = \sum_{i=0}^{\infty} a_i x^i$ with almost every $a_i = 0$. With this form we see elements of $R[X]$ are in a bijective correspondence with finite support tuples from $R^{\mathbb{N}}$.

We see $R[X]$ forms a ring with two polynomials $f, g \in R[X]$ as defined earlier having sum

$$(f + g) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and for an $\alpha \in R$

.