1. More on the Chinese Remainder Theorem

We begin by recalling this theorem, proven in the preceding lecture.

**Theorem 1.1** (Chinese Remainder Theorem). Let $R$ be a ring with ideals $I_1, I_2, \ldots, I_r$, and define a map

$$\varphi : R \rightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_r,$$

$$x \mapsto (x + I_1, x + I_2, \ldots, x + I_r).$$

Then $\varphi$ is an isomorphism if and only if: (a) $I_i + I_j = R \forall i \neq j$ and (b) $I_1 \cap I_2 \cap \cdots \cap I_r = (0)$.

Note that (a) ensures surjectivity, while (b) ensures injectivity. We will now consider an example, which recovers the usual statement of the Chinese Remainder Theorem.

**Example 1.2.** Take $n_1, n_2, \ldots, n_r \in \mathbb{Z}$, such that $\gcd(n_i, n_j) = 1 \forall i \neq j$, and set $n = n_1 n_2 \ldots n_r$ and $\bar{n}_i = n_i + (n) \in \mathbb{Z}/(n)$.

Then, working in $\mathbb{Z}/(n)$, consider $(\bar{n}_i)$ for each $i$. Now, we have:

(a) $(\bar{n}_i) + (\bar{n}_j) = \mathbb{Z}/(n)$ for $i \neq j$ and (b) $(\bar{n}_1) \cap (\bar{n}_2) \cap \cdots \cap (\bar{n}_r) = (0)$.

The first is true because $\gcd(n_i, n_j) = 1$ implies that $(n_i) + (n_j) = \mathbb{Z}$, which can be reduced mod $n$. The second is true because anything in the intersection is surely a multiple of $n$.

Hence, the Chinese Remainder Theorem claims that:

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_r).$$

Now, given any system of simultaneous congruencies $x \equiv a_i \pmod{n_i}$, with $a_i \in \mathbb{Z}$, we can consider $\bar{a}_i \in \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_2)$ and from the isomorphism produce a unique $\bar{x} \in \mathbb{Z}/(n)$ that is its preimage. Then $x \in \mathbb{Z}$ is a solution to the system of congruencies, and furthermore, any other solution differs from $x$ by a multiple of $n$.

*Date: 15 March, 2016.*
This means that we have recovered the standard Chinese Remainder Theorem from the much more general result proven in the previous lecture.

2. More operations on ideals

Here we consider the action of ring homomorphisms on ideals.

For any ring homomorphism \( f : R \to S \) and ideals \( I < R \) and \( J < S \), \( f^{-1}(J) \) is an ideal in \( R \), but \( f(I) \) is not necessarily one in \( S \).

This motivates the following pair of definitions:

**Definition 2.1.** Let \( f : R \to S \) be a ring homomorphism and \( I < R \) and \( J < S \) be ideals. Then we call \( f^{-1}(J) \) the *contraction* of \( J \), denoted \( J^c \), and the *extension* of \( I \) is \( (f(I)) < S \), for which we write \( I^e \).

In general, contractions are “nicer” and better behaved than extensions. This is already implicit in the definition, but as an example, we consider how these operations affect primeness.

**Exercise 2.2.** Suppose \( p < S \) is prime. Then \( p^e \) is prime in \( R \).

*Proof.* Suppose \( ab \in p^e \). This means that \( f(ab) \in p \), so \( f(a)f(b) \in p \). Because \( p \) is prime, it follows that either \( f(a) \in p \), in which case \( a \in p^c \), or \( f(b) \in p \), which would mean that \( b \in p^c \). \( \Box \)

Extensions, however, do not preserve primeness, as the following example demonstrates.

**Example 2.3.** Consider the inclusion map \( f : \mathbb{Z} \hookrightarrow \mathbb{Z}[i] \). We know that the non-zero prime ideals of \( \mathbb{Z} \) are those generated by prime integers. However, not all of their extensions are prime in \( \mathbb{Z}[i] \). In fact, we have the following result:

**Proposition 2.4.** Let \( p \in \mathbb{Z} \) be prime. Then \( (p)^e \) is a prime ideal in \( \mathbb{Z}[i] \) if and only if \( p \equiv 3 \pmod{4} \).

*Proof.* Note that \( \mathbb{Z}[i] \) is a Unique Factorisation Domain so every ideal is principal, and the ideal \( (x) \) is prime if and only if \( x \) is prime, which is true if and only if \( x \) is irreducible.

We proceed with three cases:

*Case 1* \( (p = 2) \). \( (2) < \mathbb{Z}[i] \) is not prime, because \( 2 = -i(1 + i)^2 \) is not irreducible.
Case 2 \((p \equiv 1 \pmod{4})\). By Gauss’ §108, there exists \(a \in \mathbb{Z}\) such that \(a^2 \equiv -1 \pmod{p}\) if and only if \(p \equiv 1 \pmod{4}\) or \(p = 2\).\(^1\) As such, \(p \mid a^2 + 1 = (a + i)(a - i)\) (in \(\mathbb{Z}[i]\)).

Now, if \(p\) is prime, then either \(p \mid (a + i)\) or \(p \mid (a - i)\). However, in either case, that would require \(p \mid 1\), which is clearly absurd.

As such, \((p) < \mathbb{Z}[i]\) is not prime.

Case 3 \((p \equiv 3 \pmod{4})\). Suppose, for a contradiction, that \(p\) is not irreducible. Then we can find non-units \(\alpha, \beta \in \mathbb{Z}[i]\) such that \(p = \alpha \beta\). This means we have \(|\alpha|, |\beta| > 1\) and \(|\alpha|^2|\beta|^2 = p^2\).

These are statements about non-negative integers, so the only possible solution is \(|\alpha| = |\beta| = p\). But then, if say \(\alpha = a + bi\), we must have \(a^2 + b^2 = p \equiv 3 \pmod{4}\), which is impossible, as all squares are congruent to either 1 or 2 \(\pmod{4}\).

It follows that \(p\) is irreducible and \((p) < \mathbb{Z}[i]\) is prime.

\[\square\]

3. Modules

Definition 3.1. Let \(R\) be a ring. An \(R\)-module \(M\) is an abelian group equipped with an \(R\)-action, that is, a map:

\[
R \times M \rightarrow M,
(r, m) \mapsto r \cdot m,
\]

that is compatible with both the ring and group structures.

That is, the action satisfies:

\[
r \cdot (m + m') = r \cdot m + r \cdot m'
(r + s) \cdot m = r \cdot m + s \cdot m
(rs) \cdot m = r \cdot (s \cdot m)
1 \cdot m = m.
\]

Remark 3.2 (Notating the action). It is sometimes useful to write the action as a map

\[
\mu : R \rightarrow \text{End}(M),
\]

\[
r \mapsto \mu(r) : M \rightarrow M,
\]

\[
m \mapsto r \cdot m.
\]

\(^1\)From the Disquisitiones. Here we need only the "if" half and \(a = (\frac{p-1}{2})!\) works.
Here \( \text{End}(M) \) is the ring of abelian group homomorphisms from \( M \) to \( M \). The notation is due to the fact that such maps are (particular) \textit{endomorphisms}.

**Definition 3.3.** Let \( M \) and \( N \) be \( R \)-modules. Then an \textit{\( R \)-module homomorphism} is an abelian group homomorphism \( \varphi : M \rightarrow N \) such that \( \varphi(r \cdot m) = r \cdot \varphi(m) \).

An \textit{\( R \)-module isomorphism} is an invertible \( R \)-module homomorphism. If such a morphism from \( M \) to \( N \) exists, we say that \( M \) and \( N \) are \textit{isomorphic as \( R \)-modules}, and can write \( M \cong N \).

**Remark 3.4.** The process through which we have just gone defines the \textit{category of \( R \)-modules}. We defined a collection of objects, and then the maps (category theoretically, \textit{morphisms}) between them. This then gives us “for free” a sense of “same-ness”.

For this reason, this is the general procedure usually followed by definitions of new “things”.

**Definition 3.5.** If \( M \) is an \( R \)-module, a \textit{submodule} of \( M \) is a subgroup \( N \subset M \) which is also closed under the \( R \)-action. That is, it satisfies:

\[ r \cdot x \in N, \forall r \in R, x \in N. \]

**Example 3.6** (\( R = k \), a field). \( k \)-modules are vector spaces over \( k \).

**Example 3.7** (\( R = \mathbb{Z} \)). \( \mathbb{Z} \)-modules are abelian groups.

**Example 3.8** (\( R = k[x] \), \( k \) a field). Let \( M \) be a \( k[x] \)-module. Then since \( k \hookrightarrow k[x] \), \( M \) is also a \( k \)-module, and accordingly a vector space over \( k \). Note that this identification means that the action of \( \alpha \in k \subset k[x] \) is necessarily scalar multiplication by \( \alpha \).

Furthermore, the action map (\( \mu \) in Remark 3.2) must assign \( x \) to some linear operator \( T \in \text{End}(M) \). This choice, together with the module axioms, determines the entire action, since we necessarily have

\[
\mu(\sum_{i=0}^{n} k_i x^i) = \sum_{i=0}^{n} k_i T^i.
\]

This means that each \( k[x] \)-module can be associated with a \( k \)-vector space, together with a privileged linear transformation. The reversibility of the association allows us to identify the two collections, that of \( k[x] \)-modules and that of pairs \((V, T)\), where \( V \) is a \( k \)-vector space and \( T \in \text{End}(V) \).
4. Operations on Modules

**Definition 4.1.** Let $M$ be an $R$-module, with some submodules $\{M_i\}$.
Then define the sum of submodules, $\sum_i M_i$, by
$$\sum_i M_i = \left\{ \sum_i m_i \mid m_i \in M_i \right\},$$
and the intersection of submodules, $\bigcap_i M_i$, as
$$\bigcap_i M_i = \{ m \mid m \in M_i \forall i \}.$$

$\sum_i M_i$ and $\bigcap_i M_i$ are both contained in $M$ as submodules, the closure in each case being given by the closure of each $M_i$.

**Definition 4.2.** Let $M$ be an $R$-module, with submodule $N$. Then
the module quotient $M/\mathcal{N}$ is defined by taking the group quotient and defining the action by
$$r \cdot (m + \mathcal{N}) = (r \cdot m) + \mathcal{N}.$$

From this definition, we have the usual isomorphism theorems, which are proven in the same way as they are for groups and rings.

**Theorem 4.3.** 1. Let $\phi : M \rightarrow N$ be an $R$-module homomorphism. Then
$$M/\ker(\phi) \cong \im(\phi).$$
2. Let $M_1$ and $M_2$ be submodules of $M$. Then
$$(M_1 + M_2)/M_1 \cong M_2/M_1 \cap M_2.$$
3. Let $L \supset M \supset N$ be $R$-modules. Then
$$L/\mathcal{N} / (M/\mathcal{N}) \cong L/M.$$

**Definition 4.4.** Let $M$ be an $R$-module, and $I < R$ an ideal. Then
we define $IM$ by
$$IM = \left\{ \sum_i r_i m_i \mid r_i \in I, m_i \in M \right\}.$$

**Exercise 4.5.** $IM$ is a submodule of $M$.

**Proof.** To show $IM$ is a subgroup, take $r, s \in IM$. Then, there exists $r_i, s_i \in I$ so that $r = \sum_i r_i m_i, s = \sum_i s_i m_i$ and because $I$ is a subgroup of $R$, $r_i - s_i \in I$ for every $i$. This means that
$$r - s = \sum_i r_i m_i - \sum_i s_i m_i = \sum_i (r_i - s_i) m_i \in IM.$$
To see $IM$ is closed under the action, take $r \in R$ and $\sum_is_im_i \in IM$. Then $r \cdot (\sum_is_im_i) = \sum_i r \cdot (s_im_i) = \sum_i(rs_i) \cdot m_i$ which is in $IM$, because $I$ is closed under multiplication by all of $R$. \hfill \Box

Notice that we needed the entire definition of $I$ as ideal in the proof, so in order for $IM$ to be a submodule, $I$ must be an ideal of $R$.

**Definition 4.6.** Let $M$ be an $R$-module. Then the annihilator of $M$ is

$$\text{Ann}(M) = \{ r \in R | r \cdot m = 0 \ \forall m \in M \}.$$  

**Exercise 4.7.** $\text{Ann}(M)$ is an ideal of $R$.

*Proof.* Let $r, r' \in \text{Ann}(M)$. Then for any $m \in M$,

$$(r - r') \cdot m = r \cdot m - r' \cdot m = 0 - 0 = 0,$$

so $(r - r') \in \text{Ann}(M)$ and the annihilator is a subgroup.

Furthermore, for any $s \in R$,

$$(sr) \cdot m = s \cdot (r \cdot m) = s \cdot 0 = 0,$$

so $(sr) \in \text{Ann}(R)$. This ensures closure under multiplication by any element of $R$, so $\text{Ann}(M)$ is an ideal of $R$. \hfill \Box