M3P8 LECTURE NOTES 10: NONCOMMUTATIVE RINGS

1. Noncommutative Rings

We now turn to the study of rings that are not necessarily commutative; we will be slightly sloppy and refer to such a ring as a "noncommutative ring" whether it is actually commutative or not.

Definition 1.1. A *noncommuative ring* R is a set together with two binary operations $+_R, \cdot_R : R \times R \to R$ (addition and multiplication) and two distinguished elements 0_R and 1_R such that:

(1) The operation $+_R$ makes R into an abelian group with identity 0_R; that is:
   - For all $r, s, t \in R$, $(r +_R s) +_R t = r +_R (s +_R t)$ (associativity of $+_R$),
   - For all $r, s \in R$, $r +_R s = s +_R r$ (commutativity of $+_R$),
   - For all $r \in R$, $r +_R 0_R = r = 0_R +_R r$ (0_R is an additive identity), and
   - For all $r \in R$, there exists an element $-r$ of R such that $r +_R (-r) = (-r) +_R r = 0_R$ (existence of additive inverses).

(2) The operation $\cdot_R$ is associative with identity 1_R:
   - For all $r, s, t \in R$, $(r \cdot_R s) \cdot_R t = r \cdot_R (s \cdot_R t)$,
   - For all $r, s \in R$, $r \cdot_R s = s \cdot_R r$, and
   - For all $r \in R$, $r \cdot_R 1_R 1_R \cdot r = r$.

(3) Multiplication distributes over addition: for all $r, s, t \in R$, $r \cdot_R (s +_R t) = r \cdot_R s +_R r \cdot_R t$ and $(s +_R t) \cdot_R r = s \cdot_R r +_R t \cdot_R r$.

As usual we will drop the subscript $_R$ in most situations.

Seeing this definition, one might wonder if it is possible to remove the hypothesis that addition is commutative as well. In fact this hypothesis is redundant: given $a, b \in R$, if one computes $(a+b)(1+1)$ using the two distributive laws, one gets:

$$(a+b)(1+1) = (a+b) + (a+b)$$

$$(a+b)(1+a) = (a+a) + (b+b)$$

depending on whether one uses distributivity on the left or right first, and thus $a + b = b + a$. The two forms of the distributive law thus force addition to be commutative.

The center of a noncommutative ring R is the set of $r \in R$ such that $rs = sr$ for all $s \in R$. It is easy to see that the center is a commutative subring of R, and that it is nonempty (in particular both 1 and 0 are in the center.)

2. Examples

The most fundamental examples of noncommutative rings are rings of matrices. Let R be any ring at all (commutative or otherwise!) and let $M_n(R)$ denote the set of n by n matrices with entries in R. We can then add and multiply elements of $M_n(R)$ using the usual rules for addition and multiplicaton of matrices, and it is not hard to verify that the ring axioms are satisfied.

Another classic example is the ring $\mathbb{H}$ of *Hamilton quaternions.* This is the ring whose elements are expressions of the form $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$ and i, j, k are fixed symbols, with multiplication defined by the following rules:

- i, j, k commute with elements of $\mathbb{R}$,
- $i^2 = j^2 = j^2 = -1$,
- $ij = -ji = k$,
- $jk = -kj = i$, and
- $ki = -ik = j$.

These rules imply that the product $(a + bi + cj + dk)(a' + b'i + c'j + d'k)$ is equal to the expression:

$$(aa'-bb'-cc'-dd')+(ab'+ba'+cd'-dc')i+(ac'-bd+ca'+db')j+(ad'+bc'-cb'+da')k$$

and one checks that the resulting multiplication is associative and distributes over addition.

By checking commutativity with i, j, and k, one verifies that the center of $\mathbb{H}$ consists of the elements $a+0i+0j+0k$, which is a subring of $\mathbb{H}$ isomorphic to $\mathbb{R}$ (and which we usually identify with $\mathbb{R}$). The action of $\mathbb{R}$ on $\mathbb{H}$ makes $\mathbb{H}$ into a four-dimensional vector space over $\mathbb{R}$, with basis $1, i, j, k$.

Note that in $\mathbb{H}$, we have $(a + bi + cj + dk) \cdot \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2} = 1$ (provided at least one of a, b, c, d is nonzero), so that every nonzero element of $\mathbb{H}$ has a multiplicative inverse. A noncommutive ring with this property is called a *division algebra* or *skew field.*

Another interesting noncommutative ring is the Weyl algebra $\mathbb{W}$ of "differential operators in one variable with polynomial coefficients". Informally, this is the noncommutive ring generated over $\mathbb{C}$ by two noncommuting elements denoted X and $\frac{d}{dx}$. These are subject to the rule $\frac{d}{dx}X = X\frac{d}{dx}+1$. (To justify this rule, think of $\frac{d}{dx}$ as representing the operation "differentiation" on smooth functions on $\mathbb{R}$, and of X as representing the operation "multiply by X". Then for any smooth function f, we have $\frac{d}{dx}Xf = X\frac{d}{dx}f + f$.)

More formally, $\mathbb{W}$ is the ring whose elements are finite formal sums $\sum a_{ij}X^i(\frac{d}{dx})^j$, with $\mathfrak{a}_{ij} \in \mathbb{C}$. To multiply two such sums, one first expands out by distributivity, using the fact that the $a_{ij} \in \mathbb{C}$ commute with X and $\frac{d}{dx}$, to obtain a sum of terms of the form $cX^{i_1}(\frac{d}{dx})^{j_1}X^{i_2}(\frac{d}{dx})^{j_2}$. If $j_1 > 0$, we use the identity $\frac{d}{dx}X = X\frac{d}{dx} + 1$ to replace such a term with

$$cX^{i_1+1}(\frac{d}{dx})^{j_1-1}X^{i_2}(\frac{d}{dx})^{j_2} + cX^{i_1}(\frac{d}{dx})^{j_1-1}X^{i_2}(\frac{d}{dx})^{j_2},$$

and repeat this process until $j_1 = 0$ (that is, until all terms are again terms of the form $cX^i(\frac{d}{dx})^j$).

The study of modules over $\mathbb{W}$ is closely related to studying certain differential equations, and provides an algebraic perspective on such questions. The elements x and $\frac{d}{dx}$ can also be interpreted as the *position* and *momentum* operators from quantum mechanics, and in fact this was one of the original motivations for introducing the Weyl algebra.

A final, fundamental example comes from group theory. Let G be a finite group, and let R be any commutative ring. The "group ring" $R[G]$ is then the set of all R-linear combinations of elements of G; that is of expressions of the form $\sum_{g\in G} r_g g$ for r_g elements of R. These are added by "combining like terms" and multiplied by the following formula:

$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{h\in G} s_h h\right) = \sum_{g,h\in G} r_g s_h gh.$$

Alternatively, one can express the sum on the right as:

$$\sum_{g\in G}\left(\sum_{h\in G} r_{gh}s_{h^{-1}}\right) g.$$

The structure of the ring $R[G]$ for various rings R (typically $R = \mathbb{C}$) is fundamental to representation theory, and provides considerable insight into the structure of the group G.

3. Ideals and modules

In the setting of noncommutative rings, the notion of ideal is slightly more subtle. In fact there are three separate notions of ideals, each of which is equivalent to the usual notion when R is commutative.

Definition 3.1. A subset I of a noncommutative ring R is a *left ideal* if I is closed under addition, and for all $i \in I$, r in R, we have $ri \in I$. Similarly, I is a *right ideal* if I is closed under addition and for all $i \in I$, r in R, we have $ir \in I$. Finally, I is a *two-sided ideal* if I is both a left ideal and a right ideal.

We will see that two-sided ideals are kernels of homomorphisms and connected with quotient rings, whereas left and right ideals are more closely connected with the module theory.

Sums and products of ideals are defined just as in the commutative world, and the (left, right, two-sided) ideal generated by a subset S of R is, as before, the smallest (left, right, two-sided) ideal containing S.

Definition 3.2. An abelian group M with a multiplication law $R \times M \to M$ is a *left R-module* if the multiplication law satisfies the rules:

(1) $r(m + m') = rm + rm'$, for $r \in R$ and $m, m' \in M$,
(2) $(r + r')m = rm + r'm$, for $r, r' \in R$ and $m \in M$,
(3) $(rr')m = r(r'm)$ for $r, r' \in R$ and $m \in M$, and
(4) $1m = m$ for all $m \in M$.

The definition of a *right R-module* is almost the same, except that property 3 reads $(rr')m = r'(rm)$ (note the reversal in order for r and r'). This is analogous to the notions of left and right actions of a group on a set.

Note that R has the structure of both a left and a right r-module over itself: as a left module its multiplication comes from multiplication by elements of R on the left, whereas its right module structure comes from multiplication by elements on the right. From this point of view a left ideal is simply a left R-submodule of R, and similarly for right ideals.

4. Homomorphisms and quotients

Definition 4.1. Let R and S be noncommutative rings. A *homomorphism* from R to S is a map $f : R \to S$ such that $f(r_1 + r_2) = f(r_1) + f(r_2)$, and $f(r_1 r_2) = f(r_1)f(r_2)$ for all $r_1, r_2 \in R$, and $f(1_R) = 1_S$.

Note that the kernel of such a homomorphism f (defined, as usual, as the set of $r \in R$ with $f(r) = 0$) is a *two-sided ideal*. Conversely, given a two-sided ideal I of R, we let R/I denote the set of equivalence classes under congruence mod I, with $(r + I)(s + I)$ defined, as usual, as $(rs + I)$. (Note that I must be a two-sided ideal for this to be well-defined; it will not be well-defined if I is merely a left or right ideal.) We have a homomorphism $r \mapsto r + I$ from R to R/I; this is, as usual, surjective with kernel I.

We also have notions of homomorphism and quotient for R-modules. In particular, if M and N are left R-modules, a homomorphism from M to N is a map $f : M \to N$ such that $f(m_1 + m_2) = f(m_1) + f(m_2)$ and $f(rm_1) = rf(m_1)$ for $m_1, m_2 \in M$ and $r \in R$. The kernel and image of such a homomorphism are left R-submodules of M and N respectively. If N is a left R-submodule of M the quotient M/N is defined in the usual way, and there is a surjective homomorphism from M to M/N with kernel N.

An *endomorphism* of a left R-module M is a homomorphism from M to M. The set of such homomorphisms is denoted $\mathrm{End}_R(M)$. It has the structure of a noncommutative ring: if $f, g : M \to M$ are endomorphisms, then the map $f + g : M \to M$ defined by $(f + g)(m) = f(m) + g(m)$ is also an endomorphism, as is the composition $f \circ g$. This makes $\mathrm{End}_R(M)$ into a noncommutative ring (with multiplication given by composition).

An important special case of this is the following, nearly trivial observation known as *Schur's Lemma*:

Lemma 4.2. *Let M be a* simple *left R-module (that is, one whose only R-submodules are M and the zero module). Then* $\mathrm{End}_R(M)$ *is a division algebra.*

Proof. Let $f \in \mathrm{End}_R(M)$ be nonzero. Then the kernel of f is not equal to M, so must be the zero submodule. Similarly the image of f must be all of M. Thus f is a bijection from M to M, and the inverse map $f^{-1} : M \to M$ is also an endomorphism of M. □