M3P8 LECTURE NOTES 2: HOMOMORPHISMS, IDEALS, AND QUOTIENTS

1. Homomorphisms

Let R and S be rings. A *homomorphism* from R to S is, roughly, a way of interpreting elements of R as elements of S, in a way that is compatible with the addition and multiplication laws on R and S. More precisely:

Definition 1.1. A function $f : R \to S$ is a homomorphism if:
(1) $f(1_R) = 1_S$,
(2) for all $x, y \in R$, $f(x +_R y) = f(x) +_S f(y)$, and
(3) for all $x, y \in R$, $f(x \cdot_R y) = f(x) \cdot_S f(y)$.

Note that if f is a homomorphism then $f(0_R) = 0_S$; this is because $f(0_R) = f(0_R +_R 0_R) = f(0_R) +_S f(0_R)$; adding the additive inverse (in S) of $f(0_R)$ to both sides gives $0_S = f(0_R)$. Thus we do not need to require this as an axiom. On the other hand we do need to require $f(1_R) = 1_S$; for certain R, S one can construct examples of maps $f : R \to S$ that satisfy properties 2) and 3) of the definition without satisfying property 1).

A bijective homomorphism $f : R \to S$ is called an *isomorphism.* In this case one verifies easily that the inverse map $f^{-1} : S \to R$ is also a bijective homomorphism.

As a first example, if R is a subring of S, then the inclusion of R into S is a homomorphism (this is just a fancy way of saying that the addition and multiplication on R are induced from the corresponding operations on S!) In particular the inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are all homomorphisms.

The composition of two homomorphisms is a homomorphism, as is easily checked from the definitions.

The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ that takes an integer m to its congruence class mod n is a ring homomorphism. In fact, this is a special case of the following construction:

Let R be any ring, and let $f : \mathbb{Z} \to R$ be a homomorphism. Then, directly from the definition, we have: $f(1) = 1_R$, $f(2) = f(1+1) = 1_R + 1_R$, etc. In particular for all $n > 0$, $f(n) = 1_R + \cdots + 1_R$, where there are n copies of 1_R in the sum. Moreover, $f(0) = 0_R$ (proved above!) and, since $0_R = f(-n+n) = f(-n) + f(n)$, we find that $f(-n)$ is the additive inverse of $1_R + \ldots 1_R$. Thus $f(n)$ is determined, for all n, completely by the fact that f is a homomorphism. In the converse direction, it is not hard to check that the map f defined above is in fact a homomorphism. We thus have:

Proposition 1.2. *For any ring R, there is a unique ring homomorphism $f : \mathbb{Z} \to R$. This homomorphism sends 0 to 0_R, a positive integer n to the* *sum of* n *copies of* 1_R*, and* $-n$ *(for* n *positive) to the additive inverse of the sum of* n *copies of* 1_R*.*

Thus, for any ring R, we can regard an integer as an element of R via this homomorphism.

2. Evaluation homomorphisms

Let R be a ring, and consider the ring $R[X]$ of polynomials in X with coefficients in R. If s is an element of R, then we can define a homomorphism: $R[X] \to R$ by "evaluation at s". More precisely, an element of $R[X]$ has the form $r_0+r_1X+\cdots+r_nX^n$ for some n. Consider the map $\phi_s : R[X] \to R$ that sends $r_0+r_1X+\cdots+r_nX^n$ to $r_0+r_1s+\cdots+r_ns^n$ (in effect, it "substitutes s for X"). It is easy to check that this is in fact a homomorphism.

More generally, if R and S are rings, $f : R \to S$ is a homomorphism, and s is an element of S, then we can define a map:

$$\phi_{f,s} : R[X] \to S,$$

by setting

$$\phi_{f,s}(r_0 + r_1X + \cdots + r_nX^n) = f(r_0) + f(r_1)s + f(r_2)s^2 + \cdots + f(r_n)s^n,$$

(that is, by applying f to the coefficients and substituting s for X.) Again, this is clearly a homomorphism.

The evaluation homomorphisms $\phi_{f,s}$ are a fundamental property of polynomial rings- in some sense, they are the reason polynomial rings are worth studying. In fact, the ring $R[X]$ is *uniquely characterized* by the fact that homomorphisms from $R[X]$ to S are in bijection with pairs (f, s), where $f : R \to S$ is a homomorphism and s is an element of S.

3. Images, kernels, and ideals

Definition 3.1. Let $f : R \to S$ be a homomorphism. The *image* of f is the set of s in S such that there exists $r \in R$ with $f(r) = s$. The *kernel* of f is the set of r in R such that $f(r) = 0$.

The image of a homomorphism from R to S is easily seen to be a subring of S. For example, if R is a subring of S, $f : R \to S$ is the inclusion and s lies in S, then the image of the map $\phi_{f,s} : R[X] \to S$ is precisely the subring $R[s]$ of S.

By contrast, the kernel of a homomorphism is almost never a subring of R (for instance, subrings contain the identity!). However, we have:

Definition 3.2. A nonempty subset I of R is an *ideal* of R if I is closed under addition, and for all elements i of I and r of R, ri is an element of I.

Then one can verify, directly from the definition, that the kernel of any homomorphism $f : R \to S$ is an ideal of R. Any ideal of R contains 0_R, and conversely the subset $\{0_R\}$ of R is an ideal, called the *zero ideal.* A homomorphism f is injective if, and only if, its kernel is the zero ideal.

The kernel of the homomorphism: $\mathbb{Z} \to R$ is either the zero ideal, or the ideal of multiples of n in $\mathbb{Z}$ for some positive n; we say that R has *characteristic zero* or *characteristic* n, respectively. If not zero, the characteristic of R is the smallest n such that the sum of n copies of 1_R is equal to zero.

4. Ideals: examples and basic operations

If r is an element of R, then any ideal of R containing R contains any multiple sr of R, for any r in S. Conversely, one checks easily that the set $\{sr : s \in R\}$ is an ideal of R. It is known as the ideal of R generated by r, and denoted $\langle r \rangle$. An ideal generated by one element in this way is called a *principal ideal.*

Note that the ideal generated by 1_R, (or more generally by any element of R with a multiplicative inverse,) is all of R. This ideal is called the *unit ideal* of R. Since every nonzero element of a field is invertible, the only ideals of a field are the zero ideal and the unit ideal.

More generally, if S is a set of elements of R, then any ideal containing S contains all elements of the form $r_1s_1 + r_2s_2 + \cdots + r_ns_n$ for n a positive integer, $r_i \in R$, and $s_i \in S$. The set of all elements of this form is an ideal of R, known as the ideal of R generated by S, and denoted $\langle S \rangle$. It is the intersection of all the ideals of R containing S.

We will show soon that any ideal of $\mathbb{Z}$ is a principal ideal, as is any ideal of the ring $k[X]$ for any field k (you may well have seen this in last year's algebra course). On the other hand, there are rings in which not every ideal is principal; for instance, the ideal $\langle X, Y \rangle$ of $k[X, Y]$ is not a principal ideal.

Given ideals I and J there are several ways to create new ideals. It is clear, for instance, that the intersection $I \cap J$ is also an ideal. Note that if I and J are given by generators, it might be hard to find generators for the intersection (certainly it's not enough to intersect the generating sets!) The *sum* $I + J$ of I and J is the set $\{r + s : r \in I, s \in J\}$; one checks that this is an ideal. It is the smallest ideal containing both I and J, or equivalently the ideal generated by $I \cup J$. The product IJ of I and J is the ideal generated by all elements of the form rs with $r \in I$ and $s \in J$; this may be strictly larger than the set of such products. (For example, consider the product of the ideals $\langle X, Y \rangle$ and $\langle Z, W \rangle$ in $k[X, Y, Z, W]$ for k a field. This product contains $XZ + YW$, but the latter is not a product of an element in $\langle X, Y \rangle$ with an element in $\langle Z, W \rangle$. THe product of I and J is always contained in the intersection of I and J, but the two need not be equal, even in simple rings like $\mathbb{Z}$.

5. Quotients

Let R be a ring and let I be an ideal of R. If r, s are elements of R, we say that *r is congruent to s mod I* if $r - s$ is in I. This is an equivalence relation on R. We denote the equivalence class of r by $r + I$, or as $[r]_I$; it is the set $\{r + s : s \in I\}$.

Let R/I denote the set of equivalence classes on R modulo I. This set has the natural structure of a ring: the additive and multiplicative identities are $0_R + I$ and $1_R + I$, respectively, and addition and multiplication are defined by $(r+I)+(s+I) = (r+s)+I$, and $(r+I)(s+I) = (rs+I)$ respectively. One has to check that these are well defined, but this is not difficult. The ring R/I is called the *quotient* of R by the ideal I.

For example, if $R = \mathbb{Z}$ and I is the ideal generated by n, then R/I is the ring $\mathbb{Z}/n\mathbb{Z}$ that we have already seen.

There is a natural homomorphism: $R \to R/I$, defined by taking r to $r+I$. This homomorphism is surjective with kernel I. We then have:

Proposition 5.1. *Let $f : R \to S$ be a homomorphism, and suppose that the kernel of f contains I. Then there is a unique homomorphism $\overline{f} : R/I \to S$ such that for all $r \in R$, $f(r) = \overline{f}(r+I)$.*

This is called the "universal property of the quotient". For a proof, note that $\overline{f}$ is necessarily unique, as every element of R/I has the form $r + I$ for some r. We must thus show that it is well-defined and gives a homomoprhism. If $r + I = r' + I$, then r and r' differ by an element of I, so $f(r) = f(r')$ since I is contained in the kernel of f. Thus $\overline{f}$ is well-defined; checking that it gives a homomorphism is straightforward.

Note that the kernel of $\overline{f}$ in the above proposition is just the image of the kernel of f in R/I. If the kernel of f is equal to I, this image is the zero ideal and $\overline{f}$ is injective. In particular, *any* homomorphism of R to S can be thought of as an isomorphism of some quotient of R with a subring of S.

6. Prime and maximal ideals

Definition 6.1. An ideal I of R is *prime* if the quotient R/I is an integral domain. It is *maximal* if R/I is a field.

Note that as fields are integral domains, every maximal ideal is prime. The converse need not hold, of course: the zero ideal in $\mathbb{Z}$ is prime but not maximal.

Lemma 6.2. *An ideal I is prime if, and only if, for every pair of elements r, s in R such that rs is in I, either r is in I or s is in I.*

This is just a restatement of the definition: R/I is an integral domain if and only if whenever two elements $r+I$ and $s+I$ satisfy $(r+I)(s+I) = 0$ in R/I, either $r+I$ or $s+I$ is zero in R/I; this is the same as saying rs lies in I if and only if either r or s lies in I.

Lemma 6.3. *An ideal I is maximal if, and only if, the only ideals of R containing I are I and the unit ideal.*

This justifies the name "maximal" for such ideals. First suppose that R/I is a field, and that J is an ideal containing I and contained in R. Then the image of J in R/I is an ideal of R/I, so it is either the zero ideal of R/I (in which case J is contained in, and thus equal to, I) or the image of J is all of R/I, in which case J contains I and an element of $1_R + I$, so J contains 1_R and is thus the unit ideal of R. Conversely, if the only ideals of R containing I are I and the unit ideal, then for any r in $R \setminus I$, the ideal of R generated by I and r contains 1_R. We can thus write $1_R = rs + i$, where $i \in I$ and $s \in R$. This means that $s + I$ and $r + I$ are multiplicative inverses of each other in R/I, so R/I is a field.