M3P8 LECTURE NOTES 1: BASIC DEFINITIONS AND EXAMPLES

1. Rings

Recall the definition of a (commutative) ring:

Definition 1.1. A *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 and commutative 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 $r \in R$, $r \cdot_R 1_R = r$.

(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 $(s +_R t) \cdot_R r = s \cdot_R r +_R t \cdot_R r$.

There's some redundancy here, of course! I've written things this way so that one obtains the definition of a noncommutative ring simply by removing the condition that multiplication is commutative. In this course, however, all rings will be commutative. When it is clear from the context what ring we are working with, we will write 0_R and 1_R as 0 and 1, $a +_R b$ as $a + b$ and $a \cdot_R b$ as ab.

Note that some definitions of ring require $1_R \neq 0_R$; we will not do this. However, it's not hard to see that if $1_R = 0_R$, then R is the one-element ring $\{0_R\}$: we certainly have $r = 1_R \cdot_R r = 0_R \cdot_R r$. On the other hand

$$0_R \cdot_R r = (0_R +_R 0_R) \cdot_R r = 0_R \cdot_R r +_R 0_R \cdot_R r,$$

and subtracting $0_R \cdot_R r$ from both sides we find that $0_R \cdot_R r = 0_R$.

Definition 1.2. A ring R is a *field* if $1_R \neq 0_R$ and every nonzero element of r has a multiplicative inverse; that is, for every $r \in R \setminus \{0_R\}$ there exists $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1_R$.

We do not consider the zero ring $\{0_R\}$ to be a field.

We've seen many examples of rings at this point. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all rings with their usual notion of addition and multiplication; all of them but $\mathbb{Z}$ are in fact fields.

As another example, we have the ring $\mathbb{Z}/n\mathbb{Z}$ of integers mod n: let $n > 0$ be an integer, and recall that a and b are said to be *congruent mod n* if $a - b$ is divisible by n. It is easy to check that this is an equivalence relation on $\mathbb{Z}$; moreover, since any integer a can uniquely be written as $qn + r$ with q, r integers and $0 \leq r < n$, the set $\{[0]_n, [1]_n, \dots, [n-1]_n\}$ is a complete list of the equivalence classes under this relation, where $[a]_n$ denotes the set of all integers congruent to a mod n. We denote this n-element set by $\mathbb{Z}/n\mathbb{Z}$, and we can define additon and multiplication in $\mathbb{Z}/n\mathbb{Z}$ by setting $[a]_n + [b]_n = [a+b]_n$ and $[a]_n[b]_n = [ab]_n$. This defines a ring structure on $\mathbb{Z}/n\mathbb{Z}$ (once one checks that it is well-defined!). This is the first example of a general construction we'll see more of later: the quotient of a ring by an ideal.

2. Polynomial rings

A very important class of rings that we'll study are the polynomial rings. Let R be any ring. Then we can form a new ring $R[X]$, called the *ring of polynomials in X with coefficients in R*. Informally, element of $R[X]$ is an expression of the form $r_0 + r_1X + r_2X^2 + \dots r_nX^n$ for some nonnegative integer n and $r_0, \dots, r_n$ in R. If $n > m$, we consider $r_0 + r_1X + r_2X^2 + \dots r_nX^n$ to represent the same element of $R[X]$ as $s_0 + s_1X + \dots s_mX^m$ if $r_i = s_i$ for $i \leq m$ and $r_i = 0_R$ for $i > m$ (that is, you can "pad out" a polynomial with terms of the form 0_RX^m without changing it.)

From a formal standpoint, it's better to define a polynomial to be an *infinite* sum $r_0 + r_1X + r_2X^2 + (\dots)$ in which *all but finitely many r_i are zero*. This makes it easier to define addition and multiplication.

The *degree* of such an expression is the largest i such that r_i is nonzero.

We add and multiply in $R[X]$ just as we would any other polynomials:

$$\sum r_iX^i +_{R[X]} \sum s_iX^i = \sum (r_i + s_i)X^i$$

and

$$\sum r_iX^i \cdot_{R[X]} \sum s_iX^i = \sum_{n=0}^{\infty} (\sum_{i=0}^{n} r_{n-i} \cdot_R s_i)X^n.$$

What about polynomial rings in more than one variable? Since the construction of polynomial rings takes an arbitrary ring as input, one can iterate it: start with a ring R, and consider first the ring $R[X]$ and then the ring $(R[X])[Y]$. An element of this has the form $\sum_i(\sum_j r_{ij}X^j)Y^i$. On the other hand, we can consider the ring $(R[Y])[X]$, whose elements have the form $\sum_j(\sum_i r_{ij}Y^i)X^j$.

Alternatively, we could consider the ring $R[X, Y]$ whose elements are formal expressions of the form $\sum_{i,j} r_{ij}X^jY^i$ with only finitely many nonzero coefficients and define addition and multiplication in the usual way. It's not hard to see that all three approaches yield "the same" ring: if we identify the element $\sum_i(\sum_j r_{ij}X^j)Y^i$ of $(R[X])[Y]$ with the element of $\sum_j(\sum_i r_{ij}Y^i)X^j$ of $(R[Y])[X]$ and the element $\sum_i\sum_j r_{ij}X^jY^i$ of $R[X,Y]$ we see that addition and multiplication in any of these three rings gives "the same" answer. We'll therefore primarily use notation like $R[X,Y]$ for polynomial rings in multiple variables, but we'll occasionally need to know that this is "the same" as $(R[X])[Y]$ or $(R[Y])[X]$. The identifications we've made here are an example of an "isomorphism of rings"- a notion we'll make precise later!

3. Subrings and Extensions

A *subring* of a ring R is a subset of R that contains 0_R and 1_R and is closed under addition and multiplication, and taking additive inverses. For example, $\mathbb{Z}$ is a subring of $\mathbb{R}$, which is itself a subring of $\mathbb{C}$. Subrings inherit the additive and multiplicative structures from the ring that contains them, and are thus themselves rings. It's easy to see that the intersection of two subrings of R (or even an arbitrary collection of subrings of R) is also a subring of R.

Now let R be a subring of S, and let α be an element of S. We can then form a subring $R[\alpha]$ of S, called the subring of S generated by α over R, as follows: an element of S lies in $R[\alpha]$ if, and only if, it can be expressed in the form $r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_n\alpha^n$ for some integer $n \neq 0$ and some elements $r_0, \ldots, r_n$ of R. Then $R[\alpha]$ is closed under addition and multiplication. This operation is known as *adjoining* the element α to the ring R.

For example, let i denote a square root of -1 in $\mathbb{C}$, and consider the subring $\mathbb{Z}[i]$ of $\mathbb{C}$. This consists of all complex numbers that can be expressed as polynomials in i with integer coefficients. Note that such an expression need not be unique; for instance the element $1+i$ of $\mathbb{Z}[i]$ can also be written as $2 + i + i^2$. Indeed, since $i^2 = -1$, we can express any element $a_0 + a_1i + a_2i^2 + \cdots + a_ni^n$ as $m + ni$ where $m = (a_0 - a_2 + a_4 + \ldots)$ and $n = (a_1 - a_3 + a_5 + \ldots)$ are integers. This expression is clearly unique, as the complex numbers $m + ni$ and $m' + n'i$ are equal only when $m = m'$ and $n = n'$.

If α is more complicated then the elements of $R[\alpha]$ may well be harder to describe (and indeed, a "nice" description might not exist at all!). For instance, if α is the real cube root of 2, then every element of $\mathbb{Z}[\alpha]$ can be uniquely expressed as $a_0 + a_1\alpha + a_2\alpha^2$ where a_0, a_1, a_2 are integers. The elements of $\mathbb{Z}[\frac{1}{2}]$ can be expressed as uniquely as $\frac{a}{b}$, where b is a power of 2 and a is odd unless $b = 1$. If α is a root of the polynomial $x^2 - \frac{1}{2}x + 1$ then every element of $\mathbb{Z}[\alpha]$ can be uniquely expressed as $a_0 + a_1\alpha$ where a_0, a_1 lies in $\mathbb{Z}[\frac{1}{2}]$, but there are pairs a_0, a_1 such that $a_0 + a_1\alpha$ does not lie in $\mathbb{Z}[\alpha]$ (Optional exercise: for which pairs a_0, a_1 of elements of $\mathbb{Z}[\frac{1}{2}]$ does $a_0 + a_1\alpha$ lie in $\mathbb{Z}[\alpha]$?)

An alternative way of defining the ring $R[\alpha]$ is to note that it is the smallest subring of S containing R and α; in one direction, any such subring contains every expression of the form $r_0 + r_1\alpha + \cdots + r_n\alpha^n$, with r_i in R, so any every subring of S containing R and α contains $R[\alpha]$. One can thus construct $R[\alpha]$ as the intersection of every subring of S containing R and α; since the intersection of any collecting of subrings of S is a subring of S it is clear that this intersection is equal to $R[\alpha]$ as defined above.

4. Integral domains and rings of fractions

Recall that a *zero divisor* in a ring R is a nonzero element a of R such that there exists a nonzero b in R with $ab = 0$. A ring in which there are no zero divisors is called an *integral domain.* For example, $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}/6\mathbb{Z}$ is not, as $2 \cdot 3$ is zero mod 6 even though neither 2 nor 3 is zero mod 6. If R is an integral domain, then we can form the *field of fractions* of R, denoted $K(R)$, in analogy to the way we build $\mathbb{Q}$ from $\mathbb{Z}$. More precisely, $K(R)$ is the set of equivalence classes of expressions $\frac{a}{b}$, where a, b are elements of R with b nonzero, and $\frac{a}{b}$ is equivalent to $\frac{a'}{b'}$ if $ab' = a'b$. We add and multiply elements of $K(R)$ just as we do for fractions: $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+b'a}{bb'}$ and $\frac{a}{b}\frac{a'}{b'} = \frac{aa'}{bb'}$. Then $K(R)$ is a field, and it contains R as a subring if we identify $r \in R$ with $\frac{r}{1}$ in $K(R)$.

The field $K(R)$ is in some sense the "smallest field containing R as a subring": when we talk about homomorphisms and isomorphisms, we'll be able to state this more precisely.

More generally, let S be a subset of R that contains 1_R, does not contain 0_R and is closed under multiplication; that is, if a, b are in S then so is ab. Then we define $S^{-1}R$ to be the subring of $K(R)$ consisting of all "fractions" of the form $\frac{a}{b}$ with $b \in S$. It is easy to see that this is closed under addition and multiplication, and defines a ring "in between" R and $K(R)$. For example, if $R = \mathbb{Z}$ and S is the set of powers of 2, then $S^{-1}R = \mathbb{Z}[\frac{1}{2}]$. On the other hand, if S is the set of odd integers, then $S^{-1}R$ is the set of all rational numbers of the form $\frac{a}{b}$ with b odd.

In general $S^{-1}R$ is the smallest subring of $K(R)$ containing R and $\frac{1}{b}$ for all $b \in S$; that is, it is the intersection of all the subrings of $K(R)$ containing R and $\frac{1}{b}$ for all $b \in S$.

The process of obtaining $S^{-1}R$ from R is called "localization" and is an extremely powerful tool. One can even make sense of it when R is *not* an integral domain, but one has to be more careful (the equivalence relation on fractions is trickier, for example); we won't discuss this in this course but it will be quite useful in future courses.