Contents

1 Lecture 1

1.1 Rings

Recall that an abelian group is set equipped with an operation that works like addition: you can add and subtract, it's commutative, associative and monoidal.

Definition 1.1
A set R is a ring if it is an abelian group equipped with an associative "multiplication" operation which has a unit 1, where $1a = a$ and this multiplication distributes over addition.

The smallest ring is the zero ring, where $1 = 0$ (and the only element is 0). Other examples of rings are $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, quaternions. Less obvious are the polynomial rings, e.g. $\mathbb{C}[x_1, \ldots, x_n]$ or $M_n(\mathbb{R})$ (the $n \times n$ matrices over $\mathbb{R}$) or $\mathbb{Z}[G]$ (linear combinations of elements of a group G). Even fancier is derivative ring $\mathbb{C}[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$, where x_i commutes with x_j and ∂_i commutes with ∂_j and ∂_i commutes with x_j for $i \neq j$, but $\partial_i x_i - x_i \partial_i = 1$ (this is a re-arrangement of the product rule).

Definition 1.2
Consider a commutative ring R. $I \subseteq R$ is an ideal if I is a subgroup of R (over the operation of addition) and it's closed under multiplication, e.g. for $r \in R$ and $i \in I$, $ri \in I$.

Ideals are generated by coprime elements; if they share a factor, some reduction can occur a la gcd and Bezout's. R is going to stand for a commutative ring from henceforth.

Definition 1.3
Consider a commutative ring R. R is a domain (or integral domain or entire ring) if $ab = 0 \implies a = 0$ or $b = 0$.

Definition 1.4
Consider a commutative ring R. R is a principal ideal ring (or principal ring) if every ideal is generated by 1 element.

A principal ideal domain is both a principal ring and a domain. We work towards the following result.

Theorem 1.1
Every finitely-generated module over a principal ideal domain is a direct sum of cyclic modules.

What do all of these words mean?

Definition 1.5
A module (or representation) over a ring R (or R-module) is an abelian group M combined with the operation of scalar multiplication by elements of R that distributes over addition. So for $r,s \in R, m,n \in M$, then $(r + s)(m + n) = rm + rn + sm + sn \in M$.

All vector spaces are modules over their field. The integers mod 12 is a $\mathbb{Z}$-module with integer multiplication as the scalar multiplication. Also $\mathbb{C}[x] \oplus \mathbb{C}[x]$ where $p(a, b) = (pa, pb)$. Furthermore,

A product of rings R_i, $\prod_i R_i$ is a funny object.

Definition 1.6
The product of rings $\prod_i R_i$ is the unique ring such that it has projection maps $\pi_j : \prod_i R_i \to R_j$ for any ring S with maps $f_j : S \to R_j$ there exists a unique map $f : S \to \prod_i R_i$ such that $f_j = \pi_j \circ f$.

The above property is called the universal property. The direct product of rings is just a ring where you just tuple together the ring elements to make a ring element.

The direct sum is similar, but with all the maps reversed. That is why it is sometimes called the coproduct.

Definition 1.7
An R-module A is the direct sum of R-modules M_i, $i \in I$ if there are maps $\phi_i : M_i \to A$ (reverse projections) and given a module B with maps $g_i : M_i \to B$, there exists a unique map $g : A \to B$ such that $g_i = g \circ \phi_i$.

The claim is that A is also a set of tuples, but $A = \{m \in \prod_i M_i \mid m_i = 0 \text{ for all but finitely many } i\}$

Definition 1.8
A module is cyclic if it is generated by one element. This element is called the generator. It is typically denoted as:

$$Rm = (m) = \{rm \mid r \in R\}$$

Definition 1.9
Consider an R-module M. If $m \in M$, then $\mathrm{ann}_R(m) = \{r \in R \mid rm = 0\}$.

The claim is that $Rm \cong R/\mathrm{ann}_R(m)$. Example $\mathbb{C}[x]/(x^{12} - 1)$.

Definition 1.10
A free R-module is a direct sum of copies of R as a module over R. We will denote this as $R^n = R \oplus \cdots \oplus R$.

So to classify finitely-generated modules, let's split them into free parts. Consider R as a PID and M as an R-module, then define

$$M_{\text{tors}} = \{m \in M \mid am = 0 \text{ for some } a \neq 0 \in R\}$$

to be the torsion submodule of M. One can easily check this is a submodule.

The following is an exact sequence, meaning that the image of each map is the kernel of the one after it.

$$0 \to M_{\text{tors}} \to M \to M/M_{\text{tors}} \to 0$$

We claim that M/M_{tors} is a free module. Consider $\overline{m} \in M/M_{\text{tors}}$. Then, $r\overline{m} = rm + M_{\text{tors}} \in M/M_{\text{tors}}$, which after addition shows the claim.