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 $\operatorname{ann}_R(m) = \{r \in R \mid rm = 0\}$.

The claim is that $Rm \cong R/\operatorname{ann}_R(m)$. 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.

2 Lecture 2

2.1 Unique Factorization Domains

We wish to show today that all principal ideal domains are **Unique Factorization Domains**. For this lecture, we will assume R denotes a principal ideal domain. We wish to show that for $r \in R$, r admits a unique factorization in terms of irreducible elements.

Definition 2.1
An irreducible element $i \in R$ is an element that has no divisors except $\pm$ itself and ± 1 and units.

Definition 2.2
An element $p \in R$ is prime if $rs \in (p) \implies r \in (p)$ or $s \in (p)$.

Theorem 2.1
Every prime element is irreducible.

Proof 2.1
Suppose p is prime and you could factor it as $p = ab$. By primality, a or b is divisible by p, without loss of generality this is a. Then $a = kp$ for some k, so $p = kbp$ or $(kb-1)p = 0$. Thus $kb - 1 = 0$ and $kb = 1$, so b and k must be units. Thus, p is irreducible.

The algorithm for creating this factorization is simple, if you have an irreducible element, just leave it. Otherwise it must be reducible; take that factor out and continue. Thus, to prove the claim, it's sufficient to show that this algorithm terminates. In other words, any chain of ideals has a largest element:

$$(r_1) \subset (r_2) \subset (r_3) \subset \cdots \subset (r)$$

If we have such a chain, note that it's finite by the following idea. Consider the union $\bigcup_i (r_i)$. Since this is an ideal and this is a PID, $\bigcup_i (r_i) = (r)$ for some $r \in R$. Furthermore, r must exist in one such ideal; that ideal must include (r), so it must be exactly (r). This property of all such chains of ideals being finite is called the *Noetherian* property. These kind of *Noetherian* rings are typically those that are finitely generated.

Theorem 2.2
Every irreducible element of a PID are prime.

Proof 2.2
Suppose $rs \in (p)$ for some r,$s \in R$. Suppose $p \in R$ is irreducible. Suppose $r \notin (p)$. But this means that $(r, p) \supsetneq (p)$. Since R is a PID, this means $(r, p) = (a)$ for some $a \in R$. Thus, $p = au$ for some $u \in R$ Thus, a is a unit, so $(a) = (1) = (r, p)$. That means for some x, y, we can write $1 = rx + py$. Multiplying by s, then $s = rxs + pys = (rs)x + pys$, so $s \in (p)$. Thus p is prime.

Now to proceed with the proof of factorization. By this algorithm, we know we can write $0 \neq r = \prod_{i=1}^{m} p_i^{a_i}$ as a product of primes (which are the same as irreducibles). Suppose there was another factorization $r = \prod_{i=1}^{n} q_i^{b_i}$. We claim that $\{p_i\}$ and $\{q_i\}$ (and associated exponents) are just the up to permutation and units. The proof is induction on $\sum_i a_i$: just take one of the primes on the left; it must divide one of the factors on the right by the definition of prime. Thus, divide on both sides and you reduce the a_is by 1 (perhaps you get some units as left-overs, we can ignore these).

2.2 Classification of Finitely-Generated Modules (Cont'd)

Recall the theorem we attempted to show last time.

Theorem 2.3
Suppose M is a finitely-generated module over a PID. then $M \cong \bigoplus_i M_i$, where each M_i is cyclic (generated by one element).

Multiplication by an element of a ring becomes a homomorphism on modules; in general this is a representation: which turns group elements into transformations. Recall we started the proof with the following construction. Take the torsion submodule

$$M_{\text{tors}} = \{m \in M \mid \exists r \neq 0 \in R, rm = 0\}$$

The claim is that $(M/M_{\text{tors}})_{\text{tors}} = \{0\}$, i.e. M_{tors} is torsion-free. Consider $\overline{m} \in M/M_{\text{tors}}$ such that $r\overline{m} = 0$ for some $r \neq 0$. This means that $rm \in M_{\text{tors}}$, so there exists $s \in R$ which is nonzero such that $srm = 0$. Since $m \in M_{\text{tors}}$, we're done. Consider the canonical homomorphism $M \to M/M_{\text{tors}}$. Why don't we just pick one representative from each coset? Usually this doesn't create a submodule, but it does here because the module is free.

Theorem 2.4
Any torsion-free finitely-generated module over a PID R is free (which means $\cong R^{\oplus n} = R^n$).

We first need the following lemma.

Lemma 1 *If $M \subset R^n$ is a submodule of the free module of rank n, then M is free of rank $\leq n$.* □

Definition 2.3
If $p \in R$ is prime, then $R/(p)$ is a field. Thus for any free R-module M, M/pM is a module over $R/(p)$ (in other words, a vector space). The rank of M is the rank of this vector space. Rank is well-defined for free modules. Equivalently, we can say that the rank is the maximal set of linearly independent elements that generate the module.

Clearly rank $R^n = \dim_{R/(p)} R^n/pR^n = (R/(p))^n$. Now let's prove our lemma by induction on n. If $n = 1$, then we have $M \subset R$. This means it's a principal ideal $(a) \subset R$ (as rings), but as R-modules, $(a)_{\text{module}} = aR \cong R^1$. Then for the inductive step, we know We know that $R^{n-1} \subset R^n$, so we have the exact sequence

$$0 \to R^{n-1} \to R^n \to_\phi R \to 0$$

we can rewrite this exact sequence for some $a \in R$:

$$0 \to M \cap R^{n-1} \to M \to (a) \to 0$$

Call $R^n = \bigoplus_{i=1}^n Rf_i$. Then we can decompose $m \in M$ as

$$m = \sum_{i=1}^{n} r_i f_i = \sum_{i=1}^{n-1} r_i f_i + r_n f_n$$

This means $\phi(m) = r_n$. This means $M = M \cap R^{n-1} \oplus aRf_n$. The first one is a subset of R^{n-1}, so it is a module of rank at most $n-1$ (by induction, free) and the second one is just R (so, free). Thus we get rank n.

Lemma 2 *If R is a PID and M is finitely generated over R and $M' \subset M$, then M' is finitely generated.*

Proof 2.3
There exists a surjective homomorphism $\phi : R^n \to M$ for some n, by the definition of direct sum. Call $M' \subset M$

and call $F = \phi^{-1}(M')$. By lemma, F is a free module of rank at most n and we have a surjective homomorphism from it to M'. Thus, it is generated by at most n elements.

Now we can prove the theorem. Suppose M is torsion-free that is finitely generated. Let's take a maximal set of linearly independent elements from M (note that this is always finite; if we have an increasing chain of inclusions, the module is finitely generated so there exists a finite set that contains every submodule). Call this set

$$f_1, \dots, f_n \text{ where if } \sum_n r_n f_n = 0, r_n \in R \implies \text{all } r_n = 0$$

Now $M/(f_1, \dots, f_n)$ has torsion, because if $g \in M, g \notin (f_1, \dots, f_n)$ then there exists r_i's and r such that $\sum_i r_i f_i + rg = 0$ where not all the coefficients are 0 (and r cannot be either). So $r \cdot \overline{g} = 0$. Thus, $M/(f_1, \dots, f_n)$ has all elements torsional.

Now consider all such g which are generators. This shows that if we take their r's and multiply them together to make $s \neq 0$, we can annihilate these generators and thus $sM \subset \sum_i R_i f_i \cong R^n$. But $M \cong sM$. So M is free. We claim this means that

$$M \cong M_{\text{tors}} \oplus M/M_{\text{tors}}$$

Clearly these are free modules–we just need to show that the canonical homomorphism is a splitting map, meaning it truly creates a direct sum.

Proof 2.4
Suppose $M/M_{\text{tors}} = \bigoplus_{i=1}^{n} R\overline{f}_i$ for some $f_i \in M$. Consider $\bigoplus Rf_i \subset M$, where f_i are some representatives of the barred versions. By our theorem, $\bigoplus Rf_i$ is free and $\bigoplus Rf_i \cap M_{\text{tors}} = 0$. Also, we can write $m \in M$ as $m' + m''$ with $m' \in M/M_{\text{tors}}$ and $m'' \in M_{\text{tors}}$, by the definition of quotient. Thus, the direct sum is indeed valid.

Theorem 2.5
If M has torsion and finitely generated, then M naturally splits as $M \cong \bigoplus_{\text{primes } p} M(p)$ where $M(p) = \{m \in M \mid p^k m = 0 \text{ for some } k \geq 0\}$.

Proof 2.5
There exists a nonzero element $r \neq 0 \in R$ such that $rM = 0$. In fact $M = \bigoplus_{p|r} M(p)$.