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

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

Now $M/(f_1, \ldots, f_n)$ has torsion, because if $g \in M, g \notin (f_1, \ldots, f_n)$ 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, $M/(f_1, \ldots, f_n)$ 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 $M = \bigoplus_{p|r} M(p)$.

3 Lecture 3

3.1 Classification of Finitely-Generated Modules

Recall that for a PID R and a finitely generated R-module M we showed that $M/M_{\text{tors}} = F = R^n$ is a free module. Suppose we have the exact sequence:

$$\cdots \to M \to_{\phi} N \to 0$$

this means $M \cong N \oplus \ker\phi$. We claim this is true if and only if there exists $N' \subseteq M$ such that $\phi\Big|_{N'} : N' \to N$ is an isomorphism.

Note that if $M \cong N \oplus \ker\phi$, it's clear that there exists an isomorphism that identifies a part of M and N. To show that $M \equiv N' \oplus \ker\phi$ we need to show $N' \cap \ker\phi = \{0\}$ and $N' + \ker\phi = M$. The first statement follows because $N' \cap \ker\phi = \ker\phi\Big|_{N'} = \{0\}$ since it's an isomorphism. Furthermore, for some $m \in M$, take $\sigma = \phi|_{N'}^{-1}$ (the **section** or right-inverse of ϕ) and $\sigma \circ \phi(m) = m' \in N'$. Then $\phi(m' - m) = \phi(m) - \phi(m) = 0$. Thus, $m' - m \in \ker\phi$, so $m = m' - k$ and we are done.

Going back to M, we can pick a basis to write $R^n = \bigoplus_{i=1}^n Rf_i$

$$\phi : M \to R^n, f_i' \mapsto f_i$$

$\phi(f_i') = f_i$, then $\bigoplus_{i=1}^n Rf_i' \cong R^n$ because the f_i' are linearly independent. Thus $M \cong M_{\text{tors}} \oplus R^n$.

Now, assume M is a finitely generated torsion module over R PID. Recall we defined

$$M(p) = \{m \in M \mid p^k m = 0 \text{ for some } k\}$$

Theorem 3.1
We can write such a module as a direct sum.

$$M = \bigoplus_{p \text{ prime in } R, (p) \supset \operatorname{ann}_R(M)} M(p)$$

Proof 3.1
Look at $M(p) \cap \bigoplus_{(q)\neq(p)} M(q)$. If $m \in M(p) \cap \bigoplus_{(q)\neq(p)} M(q)$, then $p^k m = 0$ and $m = \sum_{i=1}^s m_i$ where $q_i^{k_i} m_i = 0$. Then m is annihilated by $Q := \prod_{i=1}^s q_i^{k_i}$. Note that $Q \notin (p)$ because none of the $q_i \in (q_i)$. Thus $(p^k, Q) = (1)$. So we can write $1 = ap^k + bQ$ and $m = ap^k m + bQm = 0$. Thus, the disjointness condition is met.
Note that $\operatorname{ann}_R M = (a)$, since if we multiply two annihilators, then we get another annihilator (and thus end up with an ideal). Furthermore, it's not just 0, because there are the annihilators of the f_i, which we can multiply together to get an annihilator (an infinite counter-example is $M = \oplus_{i=1}^\infty \mathbb{Z}/(2^i)$) Let's factorize $a = \prod p_i^{k_i}$.
Now consider a small case of two ideals $M = M(p) \oplus M(q)$. Then $\operatorname{ann}(M(p) \oplus M(q)) = p^k q^\ell$ for some k, ℓ. Note that $p^k M \subseteq M(q)$ and $q^\ell M \subseteq M(p)$. Also, we can write $1 = bp^k + cq^\ell$, meaning $m = bp^k m + cq^\ell m \in M(q) \oplus M(p)$.
To do it in general, write $a = p^k \cdot Q$ where p and Q are coprime. Then $1 = p^k b + Qc$ and $m = bp^k m + cQm$. Note $bp^k m \in M(Q)$ and $Qcm \in M(p)$, so $m \in M(Q) \oplus M(p)$. By induction on the number of prime factors of a, we get the claim.

Finally, suppose M is a module with $\operatorname{ann} M = (p^a)$. $M = \sum_{i=1}^n Rf_i$. This means there exist some j such that $p^a f_j = 0$ but e.g. $p^{a-1} f_j \neq 0$. Call this f_j f_1.

Note that we cannot just always take a submodule and say it's a summand. For example, $\mathbb{Z}/4\mathbb{Z} f_1 \oplus \mathbb{Z}/2\mathbb{Z} f_2$ has a summand which is $\mathbb{Z}/2\mathbb{Z}$, but also $(2f_1, f_2) \cong \mathbb{Z}/2\mathbb{Z}$ is is a submodule; one can show however that this one is not a summand.

We will proceed by induction on the number of generators of M. Note $R/(p^a) \cong Rf_1$ by the annihilation properties. Let's rewrite $M = R/p^a + \sum_{i=2}^n Rf_i = R/p^a + \bigoplus_{i=1}^m Rg_i$ by the inductive hypothesis.

$$R/p^a \subset M \to_\phi M/Rf_1 \cong \bigoplus_{i=2}^n Rg_i$$

By the result at the beginning of lecture, we need that there exists σ such that $\phi\sigma = \mathrm{id}_{M/Rf_1}$.

Choose representatives $f_i \in M$ such that $g_i = \phi(f_i)$. To any choice of f_i, we can add any multiple of f_1, which would still be a representative. Note that two cyclic modules are isomorphic if they have the same annihilator (at least in a PID). Thus, $\operatorname{ann} g_i = \operatorname{ann}(b_i f_1 + f_i)$ if and only if $Rg_i \cong R(f_i + b_i f_1)$. Then the map $g_i \mapsto f_i + b_i f_1$ is exactly a right inverse of ϕ. (Note that $g_i \mapsto f_i$ is not even a homomorphism).

If $R/(p^a)$ has an ideal I, then $I = (p^c)/(p^a)$. So all these annhililators will purely be powers of p. Suppose $\operatorname{ann} f_i = (p^{k_i})$ and $\operatorname{ann} g_i = (p^{\ell_i})$. Furthermore, since ϕ is a homomorphism, if $a \in \operatorname{ann} f_i$, then $a \in \operatorname{ann} g_i$. So $\ell_i \leq k_i$. We want to choose b_i such that $\operatorname{ann}(b_i f_1 + f_i) = \operatorname{ann} g_i = (p^{\ell_i})$. To do this:

$$p^{\ell_i}(b_i f_1 + f_i) = b_i p^{\ell_i} f_1 + p^{\ell_i} f_i$$

But $\phi(p^{\ell_i} f_i) = p^{\ell_i}\phi(f_i) = p^{\ell_i} g_i = 0 \pmod{Rf_1}$, i.e. $p^{\ell_i} f_i \in Rf_1$. Thus $p^{\ell_i} f_i = up^{m_i} f_1$ for $u \in R$ coprime to p where we claim $m_i \geq \ell_i$, so picking $b_i = p^{m_i - \ell_i}$ is sufficient (the above expression evaluates to multiple of f_1). To see why this inequality is true, note an annihilator of $p^{\ell_i} f_i$ is $p^{k_i - \ell_i}$. Furthermore, the smallest annihilator of $p^{m_i} f_1$ is $k_1 - m_i$. Thus $k_i - \ell_i \geq k_1 - m_i$. Finally, $m_i \geq k_1 - k_i + \ell_i$ and by definition of the first one, we had $k_1 \geq k_i$. Thus, we have $m_i \geq \ell_i$.