MAS439/MAS6320
CHAPTER 1: MODULES

EVGENY SHINDER (BASED ON NOTES BY JAMES CRANCH)

Fields often make their properties known to us via vector spaces: we care so much about $\mathbb{R}$ at least partly because our universe looks like a three-dimensional vector space over it.

Modules offer a generalisation for commutative rings of what vector spaces do for fields. The definition is very similar to the definition of a vector space.

We define modules, submodules, homomorphisms of modules and quotient modules, and prove three Isomorphism Theorems.

1.1. **Modules and submodules.**

Definition 1.1. *Let R be a commutative ring. An R-*module *consists of an abelian group M together with a map*

$$R \times M \longrightarrow M,$$

written as $(r, m) \mapsto rm$, satisfying the following axioms:

- *for all $m \in M$, we have $1m = m$;*
- *for all $r, s \in R$ and $m \in M$, we have $(rs)m = r(sm)$;*
- *for all $r, s \in R$ and $m \in M$, we have $(r + s)m = rm + sm$;*
- *for all $r \in R$ and $m, n \in M$, we have $r(m + n) = rm + rn$.*

So we can add and subtract elements of M, and multiply them by elements of R. The reader might wonder why there are no axioms explaining that zeroes and subtraction behave nicely. It turns out they're not necessary:

Proposition 1.2. *Let R be a commutative ring and M an R-module. Then for all $m \in M$ we have $0m = 0$ and $(-1)m = -m$.*

Proof. Firstly, we have

$$1m + 0m = (1 + 0)m = 1m,$$

and so cancelling the $1m$ from both sides, we have $0m = 0$.

Secondly, we have

$$0 = 0m = (1 + (-1))m = 1m + (-1)m = m + (-1)m.$$

By taking the m to the other side, we get that $(-1)m = -m$. □

In case our ring is a field, we get nothing different:

Example 1.3. *If K is a field, then a K-module is exactly the same thing as a vector space over K.*

There is one other ring whose modules are a deeply familiar concept:

Proposition 1.4. *A $\mathbb{Z}$-module is the same thing as an abelian group.*

Date: February 8, 2016.

Proof. A $\mathbb{Z}$-module consists of an abelian group A, plus a multiplication map $\mathbb{Z} \times A \to A$ satisfying the module axioms. But these are uniquely determined by the abelian group structure.

For example,

$$5a = (1+1+1+1+1)a = 1a + 1a + 1a + 1a + 1a = a + a + a + a + a,$$

and

$$-3a = ((-1)+(-1)+(-1))a = (-1)a + (-1)a + (-1)a = -a - a - a.$$

Hence the scalar multiplication adds nothing new. □

However, we can often describe a module in terms of linear algebra concepts that we know about already:

Example 1.5. *A $\mathbb{C}[T]$-module consists of a complex vector space V equipped with a map $T : V \to V$.*

Indeed, adding and scalar multiplying by constant polynomials give us a $\mathbb{C}$-module, and multiplying by T gives the linear map.

Remark 1.6. *One nice thing about vector spaces is that they all have a basis: any K-vector space looks like K^n for some (possibly infinite) n. That's absolutely not true for modules over a general ring, as the example above shows: not every abelian group is of the form $\mathbb{Z}^n$.*

One occasionally needs to talk about subsets of modules which are modules. The definition is what you might expect:

Definition 1.7. *Let R be a commutative ring. A* submodule *of an R-module M consists of a subset of M which contains the zero element and is closed under addition and under multiplication by elements of R.*

Perhaps the most striking use of this is to rephrase something you know about already in this new language:

Proposition 1.8. *Let R be a commutative ring. Then addition and multiplication makes R into an R-module, and a submodule of R is exactly the same thing as an ideal of R.*

Proof. All the axioms of a module (in Definition 1.1) are well-known formulae for multiplication in a commutative ring, so R has the structure of an R-module.

A submodule of R is a subset closed under scalar multiplication by elements of R, and under addition and subtraction. That's exactly the same thing as an ideal of R. □

Here's a boring example of a module:

Example 1.9. *Let R be a commutative ring. Then the* trivial *module is given by the singleton set $\{0\}$, with the only possible addition and scalar multiplication.*

You can think of that as corresponding to the zero ideal, if you like.

Here's another general way of constructing modules.

Example 1.10. *Let R and S be a commutative rings, and let $f : R \to S$ be a ring homomorphism. Also, let M be an S-module. Then the formula $rm = f(r)m$ makes M into an R-module.*

1.2. **Homomorphisms of modules.**

Example 1.11. *By the above, as S is a module over itself, a ring homomorphism $f : R \to S$ makes S into an R-module, with the multiplication given by $rs = f(r)s$.*

Conceptually, I sometimes like to think of a ring homomorphism $f : R \to S$ as being a way of making S into an R-module, together with a way of multiplying all the elements of S with each other.

We can take Cartesian products of modules, though we usually choose to give it another name:

Definition 1.12. *Let R be a commutative ring, and let M and N be R-modules. We define a new R-module $M \oplus N$, the* direct sum *of M and N to consist of the abelian group $M \times N$ together with the following definition of multiplication:*

$$r(m, n) = (rm, rn) \quad \textit{(for } r \in R,\ m \in M \textit{ and } n \in N\textit{)}.$$

If we keep doing this on M, forming $M \oplus \cdots \oplus M$, we get something that deserves to be called M^n for some n (sometimes written $M^{\oplus n}$ to remind you what the operation you're repeating is called). A element of M^n can be thought of as an n-tuple $(m_1, \ldots, m_n)$ of elements of M.

This construction happens particularly frequently when M is R itself (regarded as a module over itself): we say that the resulting module R^n is a *(finitely generated) free* module over R.

There is an infinite version of these ideas, where we direct sum together infinitely many modules, but we won't need it.

The last thing I ought to talk about is the notion of a homomorphism of R-modules. I hope you can guess what this is:

Definition 1.13. *Let R be a commutative ring and let M and N be R-modules. A* homomorphism *$f : M \to N$ consists of a homomorphism of abelian groups from M to N with the property that $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$.*

Example 1.14. *If M is an R-module and M' a submodule, then the inclusion map $M' \to M$ is a module homomorphism.*

Example 1.15. *If R is a field, then a R-module homomorphism is exactly the same thing as a vector space homomorphism.*

Example 1.16. *If $R = \mathbb{Z}$, then a $\mathbb{Z}$-module homomorphism is exactly the same thing as a homomorphism of abelian groups.*

1.3. **Finitely generated modules.**

Definition 1.17. *Let R be a commutative ring and let M be an R-module. We say that elements $m_1, \ldots, m_k \in M$* generate *M if, for all $m \in M$ there are $r_1, \ldots, r_k \in R$ such that*

$$r_1 m_1 + \cdots + r_k m_k = m.$$

If there are elements $m_1, \ldots, m_k$ which generate M, we say that it is finitely generated*.*

Example 1.18. *The finitely generated free module R^n is indeed finitely generated (as we'd expect).*

In fact we can take the generators to be

$$\begin{aligned} r_1 &= (1, 0, 0, \ldots, 0, 0) \\ r_2 &= (0, 1, 0, \ldots, 0, 0) \\ &\vdots \\ r_n &= (0, 0, 0, \ldots, 0, 1) \end{aligned}$$

and then the element $r = (r_1, \dots, r_n)$ *can be written as*

$$r = r_1 m_1 + \cdots + r_n m_n.$$

Not every module is finitely generated. Here's an example:

Example 1.19. *Recall that a* $\mathbb{Z}$*-module is the same thing as an abelian group. The* $\mathbb{Z}$*-module given by* $\mathbb{R}$ *under addition is not finitely generated. To see that let* $m_1, \dots, m_k \in \mathbb{R}$ *be a finite list of real numbers. Then the set*

$$\{r_1 m_1 + \cdots + r_k m_k \mid r_1, \dots, r_k \in \mathbb{Z}\}$$

is countable. So it cannot be all of $\mathbb{R}$*, as* $\mathbb{R}$ *is uncountable. This shows that* $\mathbb{R}$ *does not admit a finite number of generators.*

Exercise 1.20. *Is* $\mathbb{Q}$ *a finitely generated* $\mathbb{Z}$*-module?*

Proposition 1.21. *An* R*-module* M *is finitely generated if and only if there exists a surjective homomorphism of* R*-modules*

$$\phi : R^n \to M$$

for some finite n*.*

1.4. **Quotient modules.** Imitating the definitions of quotient abelian groups and quotient vector spaces, we can define quotient modules.

In order to do so, let's first recall definitions and notation for quotients of abelian groups. Given an abelian group A and a subgroup B, we put an equivalence relation on A to define the quotient, setting $a \approx a'$ if there is $b \in B$ such that $a' \approx a + b$.

We write A/B for the quotient abelian group, which is the set of equivalence classes under this relation. We write $a + B$ for the equivalence class containing a if we're being formal, or simply call it a if we're being informal.

That gives us what we need to define quotient modules.

Definition 1.22. *Let* R *be a commutative ring, let* M *be an* R*-module and let* N *be a submodule of* M*. The* quotient module M/N *has objects consisting of the quotient abelian group* M/N*, with multiplication defined by the multiplication structure on* M*.*

Note that the multiplication is well-defined: if we have $m \approx m'$ in M, then $m' = m + n$ for some $n \in N$. Then

$$rm' = r(m + n) = rm + rn,$$

and $rn \in N$ since N is a submodule of M, so $rm' \approx rm$.

The standard examples are that if R is a field, then quotient modules are simply quotient vector spaces, while if R is $\mathbb{Z}$, then quotient modules are simply quotient abelian groups.

The following are the standard results explaining the good behaviour of quotient modules:

Theorem 1.23 (First isomorphism theorem)**.** *Let* R *be a commutative ring. Let* M *and* N *be* R*-modules, and let* $\phi : M \to N$ *be a homomorphism between them. Then:*

1. *the kernel* $\operatorname{Ker}(\phi)$ *is a submodule of* M*,*
2. *the image* $\operatorname{Im}(\phi)$ *is a submodule of* N*, and*
3. *there is an isomorphism* $\operatorname{Im}(\phi) \simeq M/\operatorname{Ker}(\phi)$*.*

Proof. The kernel is a subgroup of M because ϕ is an abelian group homomorphism. It's closed under multiplication by R since if $f(m) = 0$, then $\phi(rm) = r\phi(m) = r0 = 0$ for all r, and is hence a submodule.

Similarly, the image is a subgroup of M because ϕ is an abelian group homomorphism. It's also closed under multiplication by R since $r\phi(m) = \phi(rm)$.

The isomorphism between $\mathrm{I}m(\phi)$ and $M/\operatorname{Ker}(\phi)$ is defined as follows. Given an element $n \in \mathrm{I}m(\phi)$, associate to it an element $m \in M$ such that $\phi(m) = n$ (which is possible as n is in the image). There may be several possible choices of such m. But given any two such choices m and m', we have $\phi(m-m') = \phi(m) - \phi(m') = n - n = 0$, and hence $m - m' \in \operatorname{Ker}(\phi)$, and hence equal in $M/ker(\phi)$.

Conversely to any element $m + \operatorname{Ker}(\phi)$ in $M/\operatorname{Ker}(\phi)$ we associate the element $\phi(m) \in \mathrm{I}m(\phi)$, and this is well-defined since $\operatorname{Ker}(\phi)$ is sent to zero by definition. These two can easily be seen to define inverse module maps making an isomorphism. □

Theorem 1.24 (Second isomorphism theorem)**.** *Let R be a commutative ring. Let M be an R-module, and let S and T be submodules of M. Then:*

(1) *the set*
$$S + T = \{s + t \mid s \in S, t \in T\}$$
is a submodule of M containing S and T as submodules,
(2) *the intersection $S \cap T$ is a submodule of S, and*
(3) *there is an isomorphism $(S + T)/T \simeq S/(S \cap T)$.*

Proof. The set $S + T$ is a subgroup of M (as proved in the isomorphism theorems for groups, for example). It is closed under multiplication by R as, if $s \in S$ and $t \in T$ then $r(s+t) = rs+rt \in S+T$. Hence it is indeed a submodule of M, and it contains S (as elements of the form $s + 0$) and T (as elements of the form $0 + t$).

The set $S \cap T$ is clearly a subgroup of S, and it is closed under multiplication by R (as if $x \in S$ and $x \in T$, then $rx \in S$ and $rx \in T$ as S and T are submodules of M), and hence $rx \in S \cap T$.

To define an isomorphism between $(S + T)/T$ and $S/(S \cap T)$ we must define mutually inverse maps in each direction.

The map from $(S + T)/T$ to $S/(S \cap T)$ sends an element $(s + t) + T$ to $s + (S \cap T)$. This is well-defined. Indeed, suppose we have another way of writing the same element:
$$(s + t) + T = (s' + t') + T.$$
Then $(s + t) - (s' - t') \in T$. But this is equal to $(s - s') + (t - t')$. The latter bracket is clearly in T, so we have $s - s' \in T$. But $s - s'$ is also in S, so it's in $S \cap T$, and hence $s + (S \cap T)$ and $s' + (S \cap T)$ are the same element of $S/(S \cap T)$. It can now readily be checked to be a module homomorphism.

The map from $S/(S\cap T)$ to $(S+T)/T$ sends an element $s+(S\cap T)$ to $(s+0)+T$. To show that this is well-defined, suppose that we chose another representation $s'+(S\cap T)$. Then $s-s' \in S\cap T$, so in particular $(s + 0) - (s' + 0) \in T$, so their images are the same. This can also be checked to be a module homomorphism.

It's easy to see that these maps are indeed mutually inverse. If we start with $s + (S \cap T) \in S/(S \cap T)$, we get $(s + 0) + T \in (S + T)/T$ and then recover $s + (S \cap T) \in S/(S \cap T)$.

Conversely if we start with $(s + t) + T \in (S + T)/T$, we get $s + S \cap T \in S/(S \cap T)$ and then $(s + 0) + T \in (S + T)/T$. This differs from $(s + t) + T$ by $t \in T$, and is hence equal as an element of $(S + T)/T$. □

Theorem 1.25 (Third isomorphism theorem)**.** *Let R be a commutative ring. Let M be an R-module. Let N be a submodule of M, and P a submodule of N. Then:*

(i) *the quotient N/P is a submodule of the quotient M/P, and*
(ii) *there is an isomorphism $(M/P)/(N/P) \simeq M/N$.*

Proof. The first part is reasonably clear: the elements $n + P \in N/P$, where $n \in N$, are a subset of those elements $m + P \in M/P$, where $m \in M$, since N is a submodule of P.

For the second part, we define a pair of mutually inverse homomorphisms between $(M/P)/(N/P)$ and M/N.

An element of the $(M/P)/(N/P)$ is of the form $(m + P) + (N/P)$; given such an element we associate to it the element $m + N \in M/N$. We must show that this is well-defined. Suppose $(m + P) + (N/P)$ and $(m' + P) + (N/P)$ give the same element in $(M/P)/(N/P)$; then $m + P$ and $m' + P$ differ by an element of N/P; in other words $m - m' \in N$. But this says exactly that m and m' are sent to the same coset of N in M, so that this construction is well-defined.

Conversely, suppose given an element $m + N \in M/N$. We associate to it the element $(m + P) + (N/P)$. Again, it is not clear that it is well-defined. So suppose we have two different representations $m + N$ and $m' + N$ for the same element, so that $m - m' \in N$. Then $(m + P) - (m' + P) \in N/P$, so we get a well-defined element of $(M/P)/(N/P)$.

As in the above cases, it's easy to check that these constructions are module homomorphisms, and it's obvious that they're mutually inverse. □