CHAPTER 1

Introduction to Module Theory

1.1. Basic Definitions and Examples

Monday, January 8th

DEFINITION 1.1. An **R-module** (left) is a set M with:

(1) Abelian addition operation
(2) Action of R on M s.t.
   (a) $(r+s)m = rm + sm$
   (b) $(rs)m = r(sm)$
   (c) $r(m+n) = rm + rn$ — this says that r acts as a self homomorphism of the ring.
   (d) $1m = m$

   So it's an abelian group with an R-action.

We should think of elements of R as "scalars", and elements of M as "vectors".

LEMMA 1.2. *The set* $Hom(M,M) = \{homomorphisms\ \varphi : M \to M\}$ *is a ring.*

PROOF. If you have two homs, you can add them, and the product is a composition. They are associative, under addition, they form a group. And we have the distributive law:

$$\varphi(\xi + \psi) = \varphi\xi\varphi\psi.$$

You should think of it as similar to the ring of matrices. □

LEMMA 1.3. *If M is an R-module, then we have a ring homomorphism $\Phi : R \to Hom(M,M)$. And then mapping is given by $\Phi : a \to \varphi_a$ s.t. $\varphi_a(u) = au$.*

Note that there may be elements of R that act trivially, i.e. which send every element to zero.

DEFINITION 1.4. Module means left-module.

DEFINITION 1.5. Modules with $1m = m$ are **unital** modules. All modules dealt with are unital.

DEFINITION 1.6. An **R-submodule** is $N \leqslant M$ closed under the ring action ($rn \in N$).

PROPOSITION 1.7 (**The submodule criterion**). *Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if:*

(1) $N \neq \varnothing$,
(2) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$.

LEMMA 1.8. *Every R-module M has two submodules, 0 and M.*

LEMMA 1.9. *R is a module over itself, and in this case, the submodules of R are exactly the left ideals of R.*

DEFINITION 1.10. The **free module** of rank n over R is

$$R^n = \{(a_1, ..., a_n) : a_i \in R\}.$$

They are analogous to free groups. The set

$$\{(0, ..., 0, a_i, 0, ..., 0)\}$$

is the i-th component module and is a submodule of the free module.

LEMMA 1.11. *If M is an R-module and S is a subring of R with $1_S = 1_R$, then M is automatically an S-module as well.*

DEFINITION 1.12. If M is an R-module and I a two sided ideal of R, we say M is **annihilated** by I when for all $a \in I$, and for all $m \in M$ we have:

$$am = 0.$$

DEFINITION 1.13. We define the **annihilator** of M as $\text{Ann}(M) = \{a \in R : au = 0 \forall u \in M\} = \{a : aM = 0\}$. This is an ideal in R, and it is exactly the kernel of the homomorphism $\Phi : R \to Hom(M, M)$.

LEMMA 1.14. *When M is annihilated by I, we can make M into an (R/I)-module by redefining our ring action as:*

$$(r + I)m = rm,$$

which divys the distinct ring actions into cosets of the quotient ring.

LEMMA 1.15. *When I is maximal in R and $IM = 0$, M is a vector space over the field R/I.*

EXAMPLE 1.16. We give some examples of modules:

(1) The 0 module is $\{0\}$, where $a0 = 0\ \forall a$.
(2) R is an R-module.
(3) Free module of rank n, R^n as defined above.
(4) Any abelian group is a $\mathbb{Z}$-module:
$$nu = u + \cdots + u \text{ (n times)}.$$
(5) Any ideal in R is an R-module. $\forall u \in I$, $a \in R$ we have $au \in I$.
(6) (a) Let F be a field, and V an F-vector space. Let T be a linear transfomation of V. Then V is an $F[x]$-module:
$$(a_n x^n + \cdots a_1 x + a_0)u = a_n T^n(u) + \cdots + a_1 T(u) + a_0 u.$$
We have this because we let $xu = Tu$. And we can apply the same construction to any ring, and any modulo over this ring, it doesn't have to be a field.
(b) R-module, $T : M \to M$ is a hom-sm (as R-module, $T(au) = aT(u)$) then M is an $R[x]$-module, $xu = Tu$.
(7) Let R be a ring, X is a set, and $M = \{\text{functions } X \to R\}$.
Then M is an R-module, $(af)(x) = a(f(x))$. In this case we call M an algebra.

DEFINITION 1.17. If A is an R-module, and A is a ring itself with $a(uv) = (au)v = u(av)$ $\forall a \in R$ and $\forall u, v \in A$, then A is called an R**-algebra**.

LEMMA 1.18. *If R is a commutative ring, then $\{$functions $X \to R\}$ and R^n are R-algebras.*

Also $M_n = \{n \times n \text{ matrices over } R\}$ is a (noncommutative) R-algebra. (Why?)
If R is a subring of a ring A and $R \subset Z(A)$, then A is an R-algebra. Or: if R, A are rings and $\varphi : R \to A$ is a hom-sm with $\varphi(R) \subset Z(A)$, then again A is an R-algebra, $au = \varphi(a)u$.

LEMMA 1.19. *For any ideal I of a ring R, R is an I-algebra.*

Constructions:

(1) Submodule: a subgroup $N \subset M$ s.t. $RN \subset N$.
(2) S is a subring of R and M is an R-module, then $M$is an S-module **(reduction of scalars)**.
(3) M is an R-module, then M is an $R/\text{Ann}(M)$-module.

$$\overline{a}u = au, \overline{a} = a + \text{Ann}(M).$$

Tuesday, January 9th

Recall we noted that if we don't have the condition that $1u = u$. Assume that we don't have this condition. Let M be an R-module without it. Then define:

$$M_0 = \{u \in M : 1u = 0\},$$

$$M_1 = \{u \in M : 1u = u\}.$$

We can check that both of these are submodules of M. $\forall c \in R$, if $u \in M_0$, then $1 \cdot (cu) = c(1u) = 0$, so $cu \in M_0$. And if $u \in M_1$, then $1(cu) = c(1u) = cu$, so $cu \in M_1$. So we have checked that the definition of submodule is satisfied. Also note that $M_0 \cap M_1 = 0$.
And $\forall u \in M$, $u = 1u + (u - 1 \cdot u)$. The stuff on the right side of plus sign is in M_0 and left side is in M_1. So we have $M = M_0 \oplus M_1$.
So $\forall c \in R$, $\forall u \in M_0$, $cu = c \cdot 1u = 0$. So the above statement just says that each element in M can be written as a sum of elements from M_0, M_1.

Keep in mind that what we defined yesterday was a left module. A right module is an abelian group M with mapping $M \times R \to M$ where $(u, a) \to ua$ s.t. we have:

(1) $(u + v)a = ua + va$
(2) $(u(a + b) = ua + ub$
(3) $u(ab) = (ua)b$
(4) $u1 = u$

So note that the first two conditions are unchanged in nature from left modules, since it doesn't matter on which side you multiply the scalar (a). But the third condition is different, because we are now using a right group action. In the left module we first multiplied b by u and then a. Here we do a first, because right group action.

LEMMA 1.20. *If R is commutative, then left modules are right modules because we apply commutativity to the difference described above in the third condition.*

LEMMA 1.21. *Left ideals in R are left R-modules, and same for right.*

DEFINITION 1.22. A **two-sided R-module** is an abelian group with both left and right module structures.

Note that a two-sided ideal is an example of a two-sided module. We will only deal with commutative rings forever, and we assume that our modules are left modules, except maybe when we discuss tensor products.

REMARK 1.23. There are 2 definitions of **annihilators** in module theory. The first is the one used to define $\mathrm{Ann}_R(N)$ where N is a submodule of an R-module M, where we allow $N = M$. This is Definition 1.13. The second is the definition of the annihilator of an ideal in a module, given in Exercise 10 below, which is:

$$Ann_M(I) = \{m \in M : am = 0, \forall a \in I\}.$$

REMARK 1.24. If $N \subseteq M$, for some R-module M, then N is always a left-ideal, but not necessarily two sided, this requires N to be a submodule. But if R is commutative, this is unimportant since left ideals are right ideals.

We define the annihilator of a subset $S \subseteq R$.

DEFINITION 1.25.

$$Ann_M(S) = \{u \in M : su = 0, \forall s \in S\}.$$

The annihilator above is an additive subgroup, but not a submodule, we need S to be a **right** ideal in order to get a submodule, since we need $S(cu) = 0$, so we need $Sc \subseteq S$. Also, it is a submodule if R is commutative.

REMARK 1.26. If R is commutative, annihilators of subsets of R in M are submodules, and annihilators of subsets of M in R are two-sided ideals.

Now Professor Leibman does Exercise 10.1.11 and several others from this section.
Some particulars on the definitions of an R-algebra:

DEFINITION 1.27 (Leibman's Definition). A is an R-algebra if A is a ring and an R-module so that:

$$a(uv) = (au)v = u(av).$$

DEFINITION 1.28 (Dummit and Foote's Definition). A ring A is an R-algebra if we are given a ring homomorphism $\varphi : R \to A$ s.t. $\varphi(R) \subseteq Z(A)$, where we define the R-action on A by $au = \varphi(a)u$.

Note that if $1 \in A$, then define $\varphi : R \to A$ by $\varphi(a) = a \times 1 \in A$. Hence the two above definitions are equivalent when we have $1 \in A$. So our takeaway is that the top definition (Leibman's) is more general and just better in every way.

10.1 Exercises

1. *Prove that* $0m = 0$ *and* $(-1)m = -m$ $\forall m \in M$.

   PROOF. Suppose there exists m s.t. $0m = c \neq 0$. Then because of the group structure of our module, we have:

   $$c - c = 0 = 0m - 0m = (0 - 0)m = 0m$$

   which is a contradiction, since we assumed $0m \neq 0$.
   We add:

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

   so since $1m = m$, we know $1m+(-1)m = 0 \Rightarrow m+(-1)m = 0 \Rightarrow (-1)m = -m$. □

2. *Prove that* $R^\times$ *and* M *satisfy the two axioms in Section 1.7 for a group action of the multiplicative group* $R^\times$ *on the set* M.

PROOF. Recall that $R^\times$ denotes the group of units of R. The group action properties of a group G acting on a set X are:
(a) $g_1(g_2x) = (g_1g_2)x$,
(b) $1x = x\ \forall x \in X$.
Note that the definition of an R module stipulates that we have $(rs)m = r(sm)$ $\forall r, s \in R^\times$ and $\forall m \in M$. And another part of the definition of an R-module gives us that $1m = m\ \forall m \in M$, and since $R^\times$ is a group, we have satisfied the definition of a group action. □

3. *Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse (i.e. there is no such $s \in R$ s.t. $sr = 1$).*

PROOF. Suppose there were such an s. Then we would have:

$$srm = 1m = m = s(0) = 0,$$

which is a contradiction, since we said $m \neq 0$. □

5. *For any left ideal I of R, define:*

$$IM = \{\sum_{finite} a_i m_i : a_i \in I, m_i \in M\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

PROOF. We know IM is nonempty since I contains 0, so $0m \in IM$, and by exercise 1, we know $0 \in IM$. So let $x, y \in IM$ such that:

$$x = a_1m_1 + \cdots + a_km_k$$

$$y = b_1n_1 + \cdots + b_ln_l$$

with $a_i, b_i \in I$, $m_i, n_i \in M$, and let $r \in R$. Then we have the following by the distributive property of scalars in the definition of an R-module:

$$\begin{aligned} x + ry &= a_1m_1 + \cdots + a_km_k + r(b_1n_1 + \cdots + b_ln_l) \\ &= a_1m_1 + \cdots + a_km_k + rb_1n_1 + \cdots rb_ln_l. \end{aligned} \tag{1.1}$$

Now since I is a left ideal, we know $rb_i \in I$ since $b_i \in I$, so $x + ry$ is a finite sum of elements of the form a_im_i and so it is in IM. Then by the submodule criterion, IM is a submodule of M. □

6. *Show that the intersection of any nonempty collection of submodules of an R-module M is a submodule.*

PROOF. Let $N = \cap N_i$ be an arbitrary collection of submodules of M. Recall from group theory that an arbitrary intersection of subgroups is a subgroups, so we know $N \leqslant M$. So we need only show that it is closed under the group action of R. So let $r \in R$, and let $n \in N$. Then $n \in N_i\ \forall i$. So $rn \in N_i\ \forall i$ since N_i is a submodule of M. But then $rn \in N$ by definition, so N is a submodule. □

7. *Let $N_1 \subset N_2 \subset \cdots$ be an ascending chain of submodules of M. Prove that $N = \cup_{i=1}^{\infty} N_i$ is a submodule of M.*

PROOF. We first prove that N is a subgroup under addition of M. It is a subset of M since it is a union of subsets of M. Since $0 \in N_1$, and $N_1 \subset N_i \ \forall i$, we know $0 \in N_i \ \forall i$, so $0 \in N$. Let $n \in N$, then $n \in N_i$ for some i, so we have $-n \in N_i \subset N$, so we have additive inverses. And let $n_1, n_2 \in N$, then $n_1 \in N_i, n_2 \in N_j$ for some i, j, and without loss of generality, we may assume $i \leqslant j$. Then $N_i \subset N_j$, so $n_1 \in N_j$, and by closure of the subgroup N_j, we know $n_1 + n_2 \in N_j \subset N$, so we have additive closure of N, hence it is a subgroup of M. Now we show that N is closed under the ring action of R. So let $r \in R$, and let $n \in N$, then $n \in N_i$ for some i, so $rn \in N_i$ since N_i is a submodule, and since $N_i \subset N$, we know $rn \in N$, so N is a submodule. □

8. *An element m of the R-module M is called a torsion element if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted:*

$$Tor(M) = \{m \in M : rm = 0 \text{ for some nonzero } r \in R\}.$$

(a) *Prove that if R is an integral domain, then $Tor(M)$ is a submodule of M (called the torsion submodule of M).*

PROOF. We know $\mathrm{Tor}(M)$ is a subset of M by its definition. We first prove it is an additive subgroup. Let $m \in \mathrm{Tor}(M)$. Then $\exists r \in R$, $r \neq 0$ s.t. $rm = 0$. Then consider $-m \in M$. From exercise 1 we know $-m = (-1)m$, so we have:

$$r(-m) = r(-1)m = (-1)rm = (-1)0 = 0,$$

since R is commutative. So we have that $-m \in \mathrm{Tor}(M)$ as well, hence we have additive inverses. We check that it has additive closure. Let $m, n \in \mathrm{Tor}(M)$. Then we have $r, s \in R$, neither being zero, s.t. $rm = 0, sn = 0$. Now consider $m + n$. We have:

$$rs(m + n) = rsm + rsn = srm + rsn = s0 + r0 = 0.$$

Since we have no zero divisors, since R is an integral domain, we know $rs \neq 0$, so $m + n \in \mathrm{Tor}(M)$, we have additive closure, and $\mathrm{Tor}(M)$ is a subgroup of M. Now we need only check that it is closed under the left action of R. So let $r \in R$ and $m \in \mathrm{Tor}(M)$. Then consider rm. We assume $r \neq 0$, since otherwise $rm = 0$ which is in our subgroup. And we know $\exists s \in R$, $s \neq 0$ s.t. $sm = 0$. Now we have $srm = rsm = r0 = 0$, so rm is in $\mathrm{Tor}(M)$. So it's a submodule. □

(b) *Give an example of a ring R and an R-module M such that $Tor(M)$ is not a submodule (consider the torsion elements in the R-module R).*
So from the previous exercise, we know we must choose some R which is not an integral domain. We consider the torsion elements in the R-module R, which are:

$$\mathrm{Tor}(R) = \{r \in R : sr = 0 \text{ for some nonzero } s \in R\},$$

but these are exactly the right zero divisors of R. We consider the ring $R = \mathbb{Z}_6 \cong \mathbb{Z}/6\mathbb{Z}$, and the module of R over itself. Note that in R, $2 \cdot 3 = 6 = 0$,

$4 \cdot 3 = 12 = 0$, and $1, 5$ are not zero divisors, so we have:

$$\mathrm{Tor}(R) = \{0, 2, 3, 4\}.$$

So note that $2, 3 \in \mathrm{Tor}(R)$ and $1 \in R$, but $2 + 1 \cdot 3 = 5 \notin \mathrm{Tor}(R)$, so by the submodule criterion, it is not a submodule.

(c) *If R has zero divisors, show that every nonzero R-module has nonzero torsion elements.*

PROOF. Suppose R has zero divisors. So $\exists r, s \in R$ nonzero such that $rs = 0$. Now let M be an R-module. We wish to show that $\exists m \in M$ s.t. $m \neq 0$, $tm = 0$ for some nonzero $t \in R$. Let $n \in M$ s.t. $n \neq 0$. Now consider $sn \in M$ and $r \in R$. Now note that $rsn = 0$ and that r and sn are both nonzero, so sn is a nonzero torsion element. □

9. *If N is a submodule of M, the annihilator of N in R is defined to be:*

$$Ann_R(N) = \{r \in R : rn = 0 \text{ for all } n \in N\}.$$

Prove that the annihilator of N in R is a two-sided ideal of R.

PROOF. Let $A = \mathrm{Ann}_R(N)$. We first show that A is an additive subgroup of R. We know it is nonempty since $0 \in A$, and it is a subset of R by construction. Now let $x, y \in A$. Consider $x(-y) = -xy$. Note $-xyn = -x(yn) = -x0 = 0$ $\forall n \in N$, so by the subgroup criterion, A is a subgroup. Let $r \in R$, $n \in N$, and $a \in A$. Observe:

$$ran = r(an) = r0 = 0,$$

$$arn = a(rn) = 0,$$

since a annihilates n, and N is closed under the action of R, so $rn \in N$, and hence a also annihilates (rn). Since our n was arbitrary, this holds for all $n \in N$. Thus $ra \in A$ and $ar \in A$, and thus $RA \subseteq A$ and $AR \subseteq A$, so since it's also an additive subgroup, A is a two-sided ideal. □

10. *If I is a right ideal of R, the annihilator of I in M is defined to be:*

$$Ann_M(I) = \{m \in M : am = 0 \text{ for all } a \in I\}.$$

Prove that the annihilator of I in M is a submodule of M.

PROOF. Since I is a right ideal, we know $Ir \subseteq I$ $\forall r \in R$. Let $A = \mathrm{Ann}_M(I)$ which we know is nonempty since $0 \in M$ since it is an abelian group, and $a0 = 0$ $\forall a \in I$. Let $m, n \in A$, let $a \in I$, and let $r \in R$. Observe:

$$a(m + rn) = am + arn = 0 + arn = (ar)n = 0,$$

since $a \in I \Rightarrow ar \in I$ (I is right ideal), hence n annihilates (ar). Thus $(m+rn) \in A$. Then by the submodule criterion, since this holds for arbitrary $m, n \in A$, $r \in R$, and A is nonempty, we know A is a submodule of M. □

11. *Let M be the abelian group (i.e. $\mathbb{Z}$-module) $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.*

(a) *Find the annihilator of M in $\mathbb{Z}$ (i.e. a generator for this principal ideal).*

Recall that $\mathrm{Ann}_{\mathbb{Z}}(M) = \{z \in \mathbb{Z} : zm = 0, \forall m \in M\}$. Observe that the least common multiple of $24, 15, 50$ is 600. We claim that this is a generator for the principal ideal given by $\mathrm{Ann}_{\mathbb{Z}}(M)$. We must only check that it is nonzero, which

is obvious, and that $600m = 0$, $\forall m \in M$. So let $m \in M$, then $m = (a, b, c)$ s.t. $a \in \mathbb{Z}/24\mathbb{Z}$, $b \in \mathbb{Z}/15\mathbb{Z}$, and $c \in \mathbb{Z}/60\mathbb{Z}$. Now observe:

$$600m = 600(a, b, c) = (600a, 600b, 600c) \equiv (0, 0, 0) = 0 \in M,$$

since $600 \equiv 0 \mod 24, 15, 50$. So $\mathrm{Ann}_{\mathbb{Z}}(M) = \langle 600 \rangle$.

(b) *Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.*

Recall that $\mathrm{Ann}_M(I) = \{m \in M : mr = 0, \forall r \in I\}$. Thus we know:

$$Ann_M(I) = \{(a, b, c) \in M : (a, b, c)\},$$

$$Ann_M(2\mathbb{Z}) = \{0, 12\} \times \{0\} \times \{0, 25\}$$

12. (a) *N is a submodule of M, $I = Ann(N)$, and $K = Ann(I)$. Then $N \subseteq K$. Give an example where $N \neq K$. We have notation for annihilator, $AnnN = N^{\perp}$.*

Note that $N \subseteq (N^{\perp})^{\perp}$. Also note that for all $a \in I$, $\forall u \in N$, $au = 0$, so $u \in I^{\perp}$. So take $M = \mathbb{Z}_6 \times \mathbb{Z}_6$, $N = \{0, 3\} \times \{0\}$, where we consider these two objects as $\mathbb{Z}$-modules (abelian groups). Note $I = N^{\perp} = 2\mathbb{Z}$. And $I^{\perp} = \{0, 3\} \times \{0, 3\}$.

(b) *I is an ideal in R. Then $I \subseteq (I^{\perp})^{\perp}$. Give an example where they are not equal.*

Take $M = \mathbb{Z}_2, I = (4)$, then $I^{\perp} = M$, but $M^{\perp} = (2)$.

13. *I - ideal in R. $M' = \{u \in M : I^k u = 0$ for some $k \in \mathbb{N}\}$. Then prove that M' is a submodule.*

Proof. For any k, let $M_k = Ann(I_k)$. Then note that $M_1 \subseteq M_2 \subseteq \cdots$. If $I \subseteq J$, then $Ann(J) \subseteq Ann(I)$. Then $M' = \bigcup_{k=1}^{\infty} M_k$ is a submodule (can be easily checked). □

18. *Let $V = \mathbb{R}^2$, and let $R = \mathbb{R}[x]$. Let x be the 2 by 2 matrix with 0,-1,1,0. And let x act on V by counterclockwise rotations by 90 degrees. Then V is an R-module. Prove that V is simple. Note that R is isomorphic to $\mathbb{C}$.*

Proof. A general rule is that submodules of V are x-invariant subspaces of V as an R-module. □

19. *Idk.*

1.2. Quotient Modules and Module Homomorphisms

Definition 1.29. Let M, N be R-modules, $\varphi : M \to N$ is an **R-homomorphism** if:

(1) $\varphi(u + v) = \varphi(u) + \varphi(v)$
(2) $\varphi(au) = a\varphi(u)$.

So it is a homomorphism of groups, and also preserves scalar mult.

Definition 1.30. If R is a field and M is then a vector space, φ is called a **linear mapping**, or a **linear transformation**.

The set of all R-hom-sms from $M \to N$ is denoted by $\mathrm{Hom}_R(M, N)$.

Definition 1.31. In the case $M = N$, hom-sms $M \to M$ are called **endomorphisms**, and:

$$\mathrm{Hom}_R(M, M) = \mathrm{End}_R(M).$$

Definition 1.32. Injective hom-sms are called **monomorphisms**.

DEFINITION 1.33. Surjective hom-sms are called **epimorphisms**.

DEFINITION 1.34. Bijective hom-sms are called **isomorphisms**.

DEFINITION 1.35. Bijective endomorphisms ($M \to M$) are called **automorphisms**.

LEMMA 1.36. *If R is a commutative ring, $Hom_R(M, N)$ is an R-module, by*

- $\varphi + \psi)(u) = \varphi(u) + \psi(u)$,
- $(a\varphi)(u) = a\varphi(u)$.

So why does it have to be commutative?

PROOF. So is $a\varphi$ a hom-sm? So consider:

$$(a\varphi)(bu) = a(\varphi(bu)) = ab\varphi(u) \neq b(a\varphi)(u) = ba\varphi(u),$$

if $ab \neq ba$, so if R is noncommutative, $a\varphi$ may not be a hom-sm. □

If R is commutative, $\mathrm{End}_R(M)$ is an R-algebra, because $(\varphi\psi)(u) = \varphi(\psi(u))$, and you also have to prove that it is a ring. Under an addition it is a group, associativity is clear, and the distributive law:

$$\varphi(\psi + \xi)(u) = \varphi(\psi(u) + \xi(u)) = \varphi(\psi(u)) + \varphi(\xi(u)) = (\varphi\psi)(u) + (\varphi\xi)(u),$$

the first equality is by definition, the second is by def of hom-sm. And we also must check that scalar multiplication is preserved to prove that it is an algebra. We have:

$$((a\varphi)\psi)(u) = (\varphi(a\psi))(u) = a(\varphi\psi)(u)$$

$$((a\varphi)\psi)(u) = (a\varphi)(\psi(u)) - a(\varphi(\psi(u)))$$

$$(\varphi(a\psi))(u) = \varphi((a\psi)(u)) = \varphi(a\psi(u)) = a\varphi(\psi(u))$$

check over these conditions, confusing And $\mathrm{Aut}_R(M)$ is a group under multiplication (compositions), which is exactly the group of units in $\mathrm{End}_R(M)$. We outline some elementary properties of modules:

(1) $0u = 0$

PROOF.

$$0u = (0 + 0)u = 0u + 0u,$$

so done. □

(2) $a0 = 0$
(3) $(-a)u = a(-u) = -au$

EXAMPLE 1.37. We give some examples of R-hom-sms:

(1) $\mathbb{Z}$-modules = abelian groups (written additively). So what are $\mathbb{Z}$-hom-sms of $\mathbb{Z}$-modules? They are of course, the hom-sms of the abelian groups. If $\varphi : G \to H$ is a group hom-sm, then $\varphi(nu) = n\varphi(u)$. For vector spaces, this is not true. Note in this case:

$$\varphi : V \to W, \varphi(u + v) = \varphi(u) + \varphi(v) \nRightarrow \varphi(cu) = c\varphi(u),$$

it only works for $\mathbb{Z}$-modules.

(2) If R is commutative, and $c \in R$, then $\varphi(u) = cu$ is an R-endomorphism of M. Note:

$$\varphi(u+v) = c(u+v) = cu + cv = \varphi(u) + \varphi(v),$$

$\forall a \in R$, $\varphi(au) = cau = acu = a\varphi(u)$.

Consider $\varphi : \mathbb{Z} \to \mathbb{Z}$ given by $\varphi(n) = 2n$. It isn't a ring hom-sm since it doesn't respect mult ($\varphi(mn) \neq \varphi(m)\varphi(n)$. **But this is** a hom-sm of $\mathbb{Z}$-modules. Why? Because $\varphi(mn) = m\varphi(n)$. Now consider the ring of polyns $R = F[x,y], \varphi : x \leftrightarrow y$. Then note φ is automorphism of R, but is not a hom-sm of R-modules. Why? because it doesn't respect multiplication by scalars, take

$$yx = \varphi(xy) \neq x\varphi(y) = xx.$$

The **kernel and image** of a hom-sm are submodules. There are no "normal" submodules, we can factorize by any of them.

Wednesday, January 10th

LEMMA 1.38. *Let $\varphi : M \to N$ be a hom-sm of R-modules. Then $ker\varphi$ and $\varphi(M)$ are submodules of M and N respectively.*

PROOF. Recall K is a submodule of M if K is a subgroup of M and $RK \subseteq K$. So we will show that the two objects in the above remark are submodules. The kernel and the image are groups, if $u \in ker\varphi$, then for any $a \in R$, $\varphi(au) = a\varphi(u) = 0$l, so au is in the kernel. If $v \in \varphi(M)$, $v = \varphi(u)$, then for any $a \in R$,

$$av = \varphi(au),$$

so $av \in \varphi(M)$. □

DEFINITION 1.39. A module M is **simple**, or **irreducible**, if it has no submodules (except 0 and itself).

There are many simple modules. We will discuss Schur's Lemma.

LEMMA 1.40 (**Schur's Lemma**). *If M, N are simple R-modules, then any R-hom-sm $\varphi : M \to N$ is either 0 or an isomorphism.*

PROOF. The kernel of φ is a submodule of M, so $ker\varphi = 0$ or $\ker\varphi = M$. $\varphi(M)$ is submodule, so it is either 0 or M. If $\ker\varphi = M$, or $\varphi(M) = 0$, then $\varphi = 0$ (obvious). Otherwise, $\ker\varphi = 0$ and $\varphi(M) = N$, so φ is an isomorphism. □

COROLLARY 1.41. *If R is commutative, and M is a simple R-module, then $End_R(M) = Hom_R(M,M)$ is a division ring.*

The only example of a **noncommutative division ring** we have is the quaternions:

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

Now we will discuss **factorization of modules**.

DEFINITION 1.42. Let M be a module, and N a submodule of M, then

$$M/N = \{a + N : a \in M\}$$

has a structure of an R-module.

Recall that you needed a two-sided ideal to get a quotient ring, but we only need a left ideal to get a quotient module.

EXAMPLE 1.43. If R is a ring, and I is a left ideal in R, then R/I is not a ring, but it is an R-module.

EXAMPLE 1.44. Consider space R of square matrices with entries in a set S, and the ideal I with zeroes in the first column and arbitrary elements in all other spots. Then R/I is the set of all first columns and is isomorphic to S^n. The ideal is left and the resulting quotient is a module, but not a ring.

Observe that M/N is an abelian group. $\overline{u} = u + N \in M/N$. Let $a \in R$, then:

$$a\overline{u} = au + aN \subset au + N = \overline{au}.$$

Or: if $v = u \mod N$, $v - u \in N$, then $av = au \mod N$, $av - au = a(v - u) \in N$. So multiplication by scalars is well defined on M/N.

THEOREM 1.45. ***Isomorphism Theorems:***

(1) If $\varphi : M \to N$ is an R-hom-sm of R-modules, then $\varphi(M) \cong M/ker\varphi$ (isomorphic as modules).

(2) Let N, K be submodules of an R-module M, then

$$N + K = \{u + v\}$$

is a submodule and $(N + K)/K \cong N/(N \cap K)$.

(3) If N is a submodule of N and K is a submodule of N, then:

$$M/N \cong \frac{(M/K)}{(N/K)}.$$

(4) Submodules of M/N are in bijection with submodules of M containing N. The correspondence is:

$$K \leftrightarrow K/N$$

where $K \subseteq M$ and $K/N \subseteq M/N$.

REMARK 1.46. $N + K$ is the smallest module containing both N and K.

10.2 Exercises

4. *A is a $\mathbb{Z}$-module. $H' = Hom(\mathbb{Z}_n, A) = ?$*

   Recall $Hom(\mathbb{Z}, A) \cong A$, since from another exercise we have $Hom(R, M) \cong M$ as R-modules, since we map $\varphi \in H$ to $\varphi(1)$. So we do the same thing. We map $\varphi \in H'$ to $\varphi(1)$. So we must have $\varphi(n) = n\varphi(1) = 0$. So $\varphi(1)$ must satisfy $n\varphi(1) = 0$. So we have $\varphi(1) \in \text{Ann}(n)$. And this map is injective, $H' \to A$. On the other hand, if $b \in A$, and $nb = 0$, then define $\varphi(\overline{k}) = bk$, $k \in \mathbb{Z}$, and $\varphi \in H'$, where $\overline{k} = k \mod n$. So, $\text{Hom}(\mathbb{Z}_n, A) \cong \{ a \in A : na = 0 \} = \text{Ann}(n)$.

   Generalization: What are $H_1 = \text{Hom}(R, M) \cong M$? And what are $H_2 = \text{Hom}(R/I, M) \cong ?$ So we must have that $H_2 \subseteq H_1$. We have:

$$H_2 = \{ u \in M : Iu = 0 \} = Ann(I).$$

   Then we map $\varphi \mapsto \varphi(1)$, and I is sent to zero.

Now $\mathrm{Hom}(R^n, M) \cong M^n$, since we map $\varphi \mapsto (\varphi(e_1), ..., \varphi(e_n))$. Or we can use the exercise from the last homework:

$$Hom(A \oplus B, M) \cong Hom(A, M) \oplus Hom(B, M),$$

since:

$$Hom(R^n, M) \cong Hom(R, M)^n \cong M^n.$$

Another one: $\mathrm{Hom}(R^n/I, M) \cong Ann(I) \subseteq M^n$, where I is an ideal in R^n.
Another one: $\mathrm{Hom}(A, B^n) \cong Hom(A, B)^n$, since we proved that $Hom(A, B \oplus C) \cong Hom(A, B) \oplus Hom(A, C)$.
Another one: $\mathrm{Hom}(R^n, R^m) \cong R^{nm}$. These are $m \times n$ matrices over R. We have a basis $e_1, ..., e_n \in R^n$ and a basis $\{ b_i \} \subseteq R^m$. So for any i, we have:

$$\varphi(e_i) = c_{1,i}b_1 + \cdots + c_{m,i}b_m.$$

And these coefficients $\{ c_i \}$ are just elements of the matrix. We have a standard basis in this module, which are matrices which are zero everywhere except for one entry, and the value of this entry is 1 (typical vector space basis over $\mathbb{R}$). We do get a different isomorphism if we change our basis, so is it canonical? It is canonical because R^n has a standard basis, and so does R^m and given these bases, we have a canonical basis for R^{nm}. If we deal with an abstract free module, we may not have a standard basis.
Another one: $\mathrm{Hom}(R, R) \cong R$ as rings. This is easy. Map $\varphi \mapsto \varphi(1)$. The checking is easy. This is actually the ring $\mathrm{End}_R(R)$. Let's check it:

$$(\varphi\psi)(1) = \varphi(\psi(1)) = \varphi(\psi(1) \cdot 1) = \psi(1)\varphi(1).$$

We have this last equality because $\varphi(1)$ is a scalar element of R and so we can take it out of ψ. And We also know $\mathrm{End}_R(R^n) \cong M_{n\times n}(R)$. Multiplication is defined so that this is a ring isomorphism.

6. *Prove that* $Hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n, m)\mathbb{Z}$.

PROOF. Let $H = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$, and let $K = \mathbb{Z}/(n, m)$. Also, let $l = \gcd(n, m)$. Then $K = \mathbb{Z}_l$. So let $\varphi \in H$. Then $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$. We note here that φ is completely determined by where it sends $1 \in \mathbb{Z}_n$, since we must have $\varphi(n \cdot 1) = \varphi(0) = 0$ by the definition of a group homomorphism, thus we must have that $n\varphi(1) = 0 \in \mathbb{Z}_m$. In order to have $n\varphi(1) = 0$, we need $\varphi(1)$ to be a multiple of m. So we need $\varphi(1)$ to be a multiple of m/l, since every prime factor in l is also in the factorization of n, so we need only the prime factors of m which are not in l, hence $\varphi(1)$ must be a multiple of m/l. Now note there are exactly l multiples of m/l in $\mathbb{Z}_m$. We denote these $a_0, ..., a_{l-1}$. So we have exactly l distinct homomorphisms in H, so we denote these $\varphi_0, ..., \varphi_{l-1}$, where $\varphi_i(1) = a_i = im/l \in \mathbb{Z}_m$. Then let $\Phi : H \to K$ be given by:

$$\Phi(\varphi_i) = i \in \mathbb{Z}_l.$$

We prove this map is an isomorphism. **Homomorphism:** Observe:

$$\Phi(\varphi_i + \varphi_j) = \Phi(\varphi_{i+j \mod l}) = i + j = \Phi(\varphi_i) + \Phi(\varphi_j) \in \mathbb{Z}_l.$$

The first equality is by the additive operation on the $\mathbb{Z}$-module H, and the other equalities follow from the definition of Φ and the additive operation on $\mathbb{Z}_l$. Since φ_i is a homomorphism of R-modules, it preserves multiplication by scalars, so we have

$z\varphi_i(1) = \varphi_i(z) = za_i$, and since $\{a_i\} \cong \mathbb{Z}_l$ as a group, we know $za_i = a_{zi \mod l}$. So we have:

$$\Phi(z\varphi_i) = zi = z\Phi(\varphi_i) \in \mathbb{Z}_l.$$

So Φ preserves scalar mult, and hence it is a homomorphism.
Surjectivity: Let $i \in \mathbb{Z}_l$. Then consider $\psi \in H$ s.t. $\psi(1) = im/l$, but this is exactly how we defined φ_i, so we know $\varphi_i = \psi$, and then $\Phi(\psi) = \Phi(\varphi_i) = i$. So Φ is surjective.
Injectivity: Let:

$$\Phi(\psi) = \Phi(\xi),$$

then since we enumerated all the elements of H, we know we must have $\psi = \varphi_i$ and $\xi = \varphi_j$ for some $0 \leqslant i, j \leqslant l-1$. Then we have:

$$\Phi(\varphi_i) = i = j = \Phi(\varphi_j) \in \mathbb{Z}_l,$$

so $i \equiv j \mod l$, but since both these numbers are between 0 and $l-1$, we know $i = j$, so $\psi = \xi$, and Φ is injective. Hence it is an isomorphism. □

9. *Let R be a commutative ring. Prove that $Hom_R(R, M)$ and M are isomorphic as left R-modules. [Show that each element of $Hom_R(R, M)$ is determined by its value on the identity of R.]*

PROOF. Recall:

$$H = \mathrm{Hom}_R(R, M) = \{\varphi : R \to M\},$$

where R and M are R-modules. Let $\varphi \in H$. Recall that from the definition of H, we know:

$$\varphi(rs + t) = r\varphi(s) + \varphi(t),$$

for all $r, s, t \in R$. So note that $\forall r \in R$, we have:

$$\varphi(r) = r\varphi(1_R),$$

hence φ is complete determined by its value on 1_R. Also observe that $\varphi(1_R) \in M$, so define a map $\Phi : M \to H$ by $\Phi(m) = \varphi_m$, where we define $\varphi_m(1_R) = m$. We prove this map is an R-module isomorphism. We first prove it is an R-module homomorphism. So let $m, n \in M$, then we have:

$$\Phi(m) + \Phi(n) = \varphi_m + \varphi_n$$

Now we prove surjectivity. So let $\psi \in H$, then $\psi(1_R) = m$ for some $m \in M$, so we know $\psi = \varphi_m$. Then note that $\Phi(m) = \varphi_m$, so Φ is surjective. □

11. *Let $A_1, A_2, ..., A_n$ be R-modules and let B_i be a submodule of A_i for each $i = 1, 2, ..., n$. Prove that:*

$$(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n).$$

PROOF. So let $A = (A_1 \times \cdots \times A_n)$, $B = (B_1 \times \cdots \times B_n)$, and $C = (A_1/B_1) \times \cdots \times (A_n/B_n)$. Note that:

$$A/B = \{\, (a_1, ..., a_n) + B \,\}.$$

We know B is a submodule of A since it is clearly a subset since each component b_i of $(b_1, ..., b_n)$ is also in A_i. Also:

$$(b_1, ..., b_n) + r(d_1, ..., d_n) = (b_1, ..., b_n) + (rd_1, ..., rd_n) = (b_1 + rd_1, ..., b_n + rd_n),$$

because of how we defined add. and mult. by R in the R -module B, and because each B_i is a submodule of A_i. Then we know A/B is an R-module since we may factorize by any submodule of A. , so we let $\varphi : A/B \to C$ be given by

$$\varphi((a_1, a_2, ..., a_n) + B) = (a_1 + B_1, a_2 + B_2, ..., a_n + B_n).$$

We prove that φ is an isomorphism.

Homomorphism: Let $(x_1, x_2, ..., x_n) + B, (y_1, y_2, ..., y_n) + B \in A/B$, then

(1.2)
$$\begin{aligned}\varphi(((x_1, x_2, ..., x_n) + B) + ((y_1, y_2, ..., y_n) + B)) &= \varphi(((x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n)) + B)\\ &= \varphi((x_1 + y_1, x_2 + y_2, ..., x_n + y_n) + B)\\ &= (x_1 + y_1 + B_1, x_2 + y_2 + B_2, ..., x_n + y_n + B_n)\\ &= (x_1 + B_1, x_2 + B_2, ..., x_n + B_n)\\ &+ (y_1 + B_1, y_2 + B_2, ..., y_n + B_n)\\ &= \varphi((x_1, x_2, ..., x_n) + B) + \varphi((y_1, y_2, ..., y_n) + B),\end{aligned}$$

by the direct product operation on A/B and C. And for multiplication, we have:

(1.3)
$$\begin{aligned}\varphi(r((x_1, ..., x_n) + B)) &= \varphi(r(x_1, ..., x_n) + B)\\ &= \varphi(rx_1, ..., rx_n) + B)\\ &= (rx_1 + B, ..., rx_n + B)\\ &= r(x_1 + B, ..., x_n + B)\\ &= r\varphi((x_1, ..., x_n) + B),\end{aligned}$$

so φ is a homomorphism.

Injection: Let $(x_1, x_2, ..., x_n) + B, (y_1, y_2, ..., y_n) + B \in A/B$, and let

(1.4)
$$\begin{aligned}&\varphi((x_1, x_2, ..., x_n) + B) = \varphi((y_1, y_2, ..., y_n) + B)\\ \Rightarrow\ &(x_1 + B_1, x_2 + B_2, ..., x_n + B_n) = (y_1 + B_1, y_2 + B_2, ..., y_n + B_n).\end{aligned}$$

So then we have that $x_i + B_i = y_i + B_i$ for all i, thus

(1.5)
$$\begin{aligned}(y_1, y_2, ..., y_n) + B &= (y_1, y_2, ..., y_n) + (B_1 \times B_2 \times \cdots \times B_n) = (y_1 + B_1 \times y_2 + B_2 \times \cdots \times y_n + B_n)\\ &= (x_1 + B_1 \times x_2 + B_2 \times \cdots \times x_n + B_n) = (x_1, x_2, ..., x_n) + B\end{aligned}$$

by the direct product operation, so φ is in injective.

Surjection: Let $(a_1+B_1, a_2+B_2, ..., a_n+B_n) \in C$. Then we must have that $a_i \in A_i$ for all i by definition of C and the quotient modules A_i/B_i, so $(a_1, a_2, ..., a_n) \in A \Rightarrow (a_1, a_2, ..., a_n)+B \in A/B$, and $\varphi((a_1, a_2, ..., a_n)+B) = (a_1+B_1, a_2+B_2, ..., a_n+B_n)$, so φ is surjective by definition. Hence φ is an isomorphism, and $A/B \cong C$. □

12. *Let I be a left ideal of R and let $n \in \mathbb{N}$. Prove:*

$$R^n/IR^n \cong R/IR \times \cdots \times R/IR$$

.

PROOF. So we use the first isomorphism theorem. We map $R^n \to (R/I)^n$ by $(a_1, ..., a_n) \mapsto (a_1 \mod I, ..., a_n \mod I) = (\overline{a_1}, ..., \overline{a_n}) \in (R/I)^n$. This is clearly surjective. And the kernel is just $I^= \{ (a_1, ..., a_n) : a_i \in I \}$. And $I^n = IR^n$, why?

PROOF. Take:

$$IR^n = \left\{ \sum b_i(a_{i,1}, ..., a_{i,n}) : b_i \in I \right\}.$$

And also take note: $(b_1, ..., b_n) \in I$ can be written as:

$$(b_1, ..., b_n) = b_1(1, ..., 0) + \cdots + b_n(0, ..., 0, 1) \in IR^n.$$

So these are the same object. □

□

1.3. Generation of Modules, Direct Sums, and Free Modules

Assume R is a unital ring, i.e. that $1 \in R$.

DEFINITION 1.47. Let M be an R-module and S be a subset of M. We say that M is **generated by** S if for any $u \in M$, there exists $v_1, ..., v_k \in S, a_1, ..., a_k \in R$ such that:

$$u = a_1v_1 + \cdots + a_kv_k,$$

which is called a **linear combination** of $v_1, ..., v_k$.

We could define it another way.

DEFINITION 1.48. Let $S \subseteq M$. Then

$$RS = \{a_1v_1 + \cdots + a_kv_k : a_i \in R, v_i \in S\}$$

is the smallest submodule of M containing S. RS is called the **submodule generated by** S**.**

REMARK 1.49. M is generated by S iff $M = RS$.

DEFINITION 1.50. The **free module generated by** S is the set of functions $f : S \to R$ s.t. $f(s) = 0$ for all but finitely many $s \in S$.

So consider the case where S is finite to simplify the discussion: If $S = \{s_1, ..., s_n\}$, the free module is $\{a_1s_1 + \cdots + a_ns_n : a_i \in R, s_i \in S\}$.

It is the direct sum of $|S|$ copies of R. Equivalently, the free module is:

$$\{a_1s_1 + \cdots + a_ns_n : a_i \in R, s_i \in S\},$$

the set of formal linear combinations of elements in S. Each element in this set corresponds to a function $f : s_i \to a_i$ and maps s to zero if $s \neq s_1, ..., s_n$. You should think of this like a free group.

The difference between the above definitions is the free generated module is the case where S is not a subset of M, it is just some random set.

Let M be an R-module, let S be a subset of M. let F be the free module generated by S, then we have a unique hom-sm $\varphi : F \to M$ s.t. $\varphi(s) = s \ \forall s \in S$.

$$\varphi(a_1s_1 + \cdots + a_ns_n) = a_1s_1 + \cdots + a_ns_n \in M.$$

On the left hand side inside φ we see a formal linear combination, the s's are just letters, we forget that they come from a subset of M. They are just symbols. On the right hand side, we are in M, so we remember that $S \subseteq M$.

EXAMPLE 1.51. Let $S = \{2, 3\} \subseteq \mathbb{Z}$. And let:

$$F = \{n \cdot 2 + m \cdot 3\} \cong \mathbb{Z}^2,$$

where in the above we see $2, 3$ as just symbols, easily replaceable by x, y. Now consider a map $F \to \mathbb{Z}$, where $n \cdot 2 + m \cdot 3 \to 2n + 3m$ and on the left hand side of this map, we then remember that $2, 3$ are numbers.

If M is generated by S, then φ is surjective, and $M \cong F/ker\varphi$.

DEFINITION 1.52. If M has a finite generated set S, then M is **finitely generated**.

REMARK 1.53. If $|S| = n$, then M is a factor module of R^n.

DEFINITION 1.54. M is called **cyclic** if it is generated by just one element, $M = Ru$ for some $u \in M$.

In this case, $M \cong R/I$, I is a left ideal in R. We have $\varphi : R \to M$ - surjective, which maps a to au, and $I = ker\varphi$ is a left ideal. Observe:

$$I = \{a : au = 0\} = \text{Ann}(u).$$

And $au = 0 \Rightarrow \forall b \in R, (ba)u = 0$, so $ba \in I$. But $ab(u) =?$

Thursday, January 11th

REMARK 1.55. When M is cyclic, we know:

$$M \cong R/I$$

where $I = \text{Ann}(u) = \{a : au = 0\}$, which is a left ideal. Recall that u is the generator of M.

LEMMA 1.56. *An abelian group G is cyclic as a $\mathbb{Z}$-module if and only if it is cyclic as a group.*

PROOF. $\exists u \in G$ s.t. $G = \mathbb{Z}u = \{nu : n \in \mathbb{Z}\}$. □

REMARK 1.57. Let M be an F-vector space, and let T be a linear transformation of M. Then M is an $F[x]$-module by $xu = Tu$, $u \in M$.

$$(a_n x^n + \cdots + a_1 x + a_0)u = a_n T^n u + \cdots + a_1 Tu + a_0 u.$$

Also, M is cyclic as an $F[x]$-module if $\exists u$ s.t. $\forall v \in M$, $\exists n, a_i$ s.t. $v = a_n T^n u + \cdots + a_1 Tu + a_0 u$.

DEFINITION 1.58. That is, if $u, Tu, T^2u, ...$ span M, then u is called a **cyclic vector** for T.

LEMMA 1.59. *For any simple module M is cyclic*

PROOF. take any nonzero $u \in M$, then Ru is a nonzero submodule, so $Ru = M$. □

Converse is not true: $\mathbb{Z}_6$ as a $\mathbb{Z}$-module is cyclic (generated by 1), but not simple (has a submodule $2\mathbb{Z}_6 = \{0, 2, 4\}$.

Every group is a factor group of a free group.

Friday, January 12th Now we'll do some exercises. Professor Leibman does Exercises 10.1.5,6 which are completed above. He defines the annihilator of a subset of M again, and proves it is a left ideal. This is Exercise 10.1.9.

Tuesday, January 16th

Take $R = F[x_1, x_2, ...]$. Consider R as a module over itself. It is generated by 1, since $R = R \cdot 1$.

Note $I = (x_1, x_2, ..)$-submodule of R, all polynomials with zero constant term.

LEMMA 1.60. *I as defined above is not finitely generated.*

PROOF. Assume that it is finitely generated. So $I = R(f_1, ..., f_k)$, for $f_i \in I$, where we assume f_i has zero constant term. Let $x_1, ..., x_n$ be all variables appearing in $f_1, ..., f_k$, then any nonzero element of $R(f_1, ..., f_k)$ (these are linear combinations of the f's) contains at least one of $x_1, ..., x_n$, since f_i has zero constant term. But I is not such, $x_{n+1} \in I$, so $I \neq R(f_1, ..., f_k)$. □

EXAMPLE 1.61. Let $R = F[x, y]$, and $I = (x, y)$. Then R is an R module, is generated by 1, and I needs at least two generators. So we can think of this as R being a one "dimensional" module, but I is not one "dimensional". Let

$$f = ax + by + g(x, y),$$

$\forall g \in R$, $gf = c(ax + by) + (\cdots)$. We are assuming $a, b \neq 0$. The linear part of I is two "dimensional". So

$$\{g \in R, gf = c(ax + by) + (\cdots)\} \neq I.$$

If $b \neq 0$, $x \notin Rf$, and if $a \neq 0$, $y \notin Rf$.

Consider $M_1 \oplus M_2 = M_1 \times M_2$ is called direct sum = direct product, for two or finitely many modules. And this direct sum has the universal repelling property (appendix A).

For $M_1, M_2, ...$

DEFINITION 1.62. Direct product $M_1 \times M_2 \times \cdots = \Pi_{i=1}^{\infty} M_i$ is

$$M = \{(u_1, u_2, ...) : u_i \in M_i\},$$

with $(u_1, u_2, ...) + (v_1, v_2, ...) = (u_1 + v_1, u_2 + v_2, ...)$. And scalar mult. is defined as one would expect.

More generally, if M_α $\alpha \in \Lambda$ are modules, then $\Pi_{\alpha \in \Lambda} = \{f : \Lambda \to \cup_{\alpha + \Lambda} M_\alpha : f(\alpha) \in M_\alpha\}$. For any α, choose $u_\alpha \in M_\alpha$.

Elements: $(u_\alpha)_{\alpha \in \Lambda}$.

Direct Sums: $M_1 \oplus M_2 \oplus \cdots = \{(u_1, u_2, ...) : u_i \in M_i, u_i = 0, \text{ for all but finitely many } i\}$. This is a subset of $M_1 \times M_2 \times \cdots$.

Another way:

$M_1 \oplus M_2 \oplus \cdots = \{u_{i_1} + u_{i_2} + \cdots + u_{i_k} : u_{i_j} \in M_{i_j}\}$. This is a submodule of $M_1 \times M_2 \times$.

For M_α, $\alpha \in \Lambda$,

$$\bigoplus_{\alpha \in \Lambda} M_\alpha = \{f : \Lambda \to \cup M_\alpha : \forall \alpha \in \Lambda, f(\alpha) \in M_\alpha, f(\alpha) = 0 \text{ for all but finitely many } \alpha\}.$$

This is a superset of $\Pi_{\alpha \in \Lambda} M_\alpha$.

Universal Properties:

R-modules M_α, $\alpha \in \Lambda$.

(1) Direct Product: Category: objects are (Module N with hom-sms $\psi_\alpha : N \to M_\alpha$, $\forall \alpha \in \Lambda$.

Morphisms: given two objects $(N_1, \psi_\alpha : N \to M_\alpha)$

$(N_2, \psi_\alpha : n \to M_\alpha)$ a morphism is a hom-sm $\varphi : N_1 \to N_2$ s.t. $\psi_\alpha = \varphi_\alpha \varphi \ \forall \alpha$. Direct product is universal attracting object.

Wednesday, January 17th

THEOREM 1.63 (**Chinese Remainder Theorem for Modules**). *Let R be a commutative unital ring, $I_1, ..., I_n$ be pairwise comaximal ideals in R:*

$$(I_i + I_j = (1), \forall i \neq j),$$

and M be a an R-module. Then the homomorphism $M \to M/I_1M \oplus \cdots \oplus M/I_nM$ given by $u \to (u \mod I_1M, ..., u \mod I_nM)$ induces an isomorphism $M/(I_1 \cdots I_n)M \to M/I_1M \oplus \cdots M/I_nM$ and $I_1M \cap \cdots \cap I_nM = (I_1 \cdots I_n)M$.

PROOF. For $n = 2$. $I_1 + I_2 = (1)$.

Define $\varphi : M \to M/I_1M \oplus M/I_2M$, where $\ker\varphi = I_1M \cap I_2M$. And there exists $a_1 \in I_1, a_2 \in I_2$ s.t. $a_1 + a_2 = 1$, since comaximal. And $\forall u \in I_1M \cap I_2M$, we have:

$$u = 1u = a_1u + a_2u.$$

So, $I_1M \cap I_2M \subseteq I_1I_2M$, since the first term in the righthand side above is in $I_1(I_2)M$ and so is the second term, by commutativity. Also, $I_1I_2M \subseteq I_2M \cap I_2M$. So $I_1I_2M = I_1M \cap I_2M = \ker\varphi$.

Surjectivity: $\forall u_1, u_2 \in M$, put $u = a_2u_1 + a_1u_2$. Then:

$$u = (1 - a_1)u_1 + a_1u_2 = u_1 + a_1(u_2 - u_1) = u_1 \mod I_1M,$$

and $u = u_2 \mod I_2M$. So $\varphi(u) = (\overline{u}_1, \overline{u}_2)$.

Now for $n \geqslant 3$, we use induction.

LEMMA 1.64. *I_1 and $I_2 \cdots I_n$ are comaximal.*

PROOF. $\forall i = 2, ..., n$, let $a_i \in I_1, b_i \in I_i$ be s.t. $a_i + b_i = 1$. Then:

$$1 = \prod(a_i + b_i) = (something) + b_2 \cdots b_n,$$

where something is in I_1 and $b_2 \cdots b_n \in I_2 \cdots I_n$. □

Then:

$$M/(I_1I_2 \cdots I_n)M \cong M/I_1 \oplus M/(I_2 \cdots I_n)M \cong \cdots \cong M/I_1M \oplus \cdots \oplus M/I_nM$$

by induction, where the last $\cong$ is under the mapping $u \to (u \mod I_1M, ..., u \mod I_nM$. □

DEFINITION 1.65. M_1, M_2 are submodules of M. M is said to be an internal direct sum $M = M_1 \oplus M_2$ if there exists a $\varphi : M \to M_1 \oplus M_2$ where we also have maps in a diamond up to M_1 and down to M_2 s.t. $\varphi|_{M_1} = Id_{M_1}$ and the same for M_2.

REMARK 1.66. We say that we have an **internal direct sum** if the above map exists. The "internal" means that we are working entirely inside a parent module M.

THEOREM 1.67. *Let M_1, M_2 be submodules of M. Then $M = M_1 \oplus M_2$ (**internal direct sum**) if and only if $\forall u \in M$ is uniquely representable in the form $u = u_1 + u_2$ s.t. $u_1 \in M_1$, $u_2 \in M_2$ if and only if $M = M_1 + M_2$ and $M_1 \cap M_2 = 0$. These are all equivalent definitions.*

Let M_α, $\alpha \in \Lambda$ be submodules of$M$. M is an (internal) direct sum of M_α:

$$M = \bigoplus_{\alpha\in\Lambda} M_\alpha,$$

if there exists an isomorphism $\varphi : M \to \bigoplus_{\alpha\in\Lambda} M_\alpha$ where the target space is the external, formal direct sum, s.t. $\varphi|_{M_\alpha} = Id_{M_\alpha}, \forall\alpha$. This is so if and only if $\forall u \in M$ is uniquely representable as $u = \sum_{i=1}^{k} u_{\alpha_i}$ for some distinct $\alpha_1, ..., \alpha_k$ where $u_{\alpha_i} \in M_{\alpha_i}, \forall i$ and if and only if $M = \sum M_\alpha$ and $\forall\alpha$, $M_\alpha \cap \sum_{\beta\neq\alpha} M_\beta = 0$.

Free Modules.

Definition 1.68. A **free module** is a direct sum of finitely or infinitely many copies of R,

$$F_\Lambda = \bigoplus_{\alpha\in\Lambda} R = \{a_{\alpha_1} + \cdots + a_{\alpha_k} : k \in \mathbb{N}, \alpha_i \in \Lambda, a_{\alpha_i} \in R\},$$

where the sum of u's above is a formal sum. We can also define it as:

$$F_\Lambda = \{(a_\alpha)_{\alpha\in\Lambda} : a_\alpha \in R, \forall\alpha, a_\alpha = 0 \text{ for all but finitely many } \alpha\}.$$

Note R is unital here.

If M is an R-module, $v_\alpha \in M, \alpha \in \Lambda$. Then there exists a unique hom-sm $\varphi : F \to M$ s.t. $\varphi(e_\alpha) = v_\alpha, \forall\alpha$ where $e_\alpha = (a_\beta)_{\beta\in\Lambda}, a_\alpha = 1, a_\beta = 0$ for $\beta \neq \alpha$. As an example, if $\Lambda = \{1, ..., k\}$, we have:

$$e_1 = (1, 0, ..., 0),$$

$$e_k = (0, ..., 0, 1).$$

Also, we say that a module M is free if $M \cong$ a free module F. This is so if any only if M has a **basis**: elements $u_\alpha, \alpha \in \Lambda$.

Thursday, January 18th

Let R be a unital ring. Recall that a **free module** is $\bigoplus_{\alpha\in\Lambda} R$. If Λ is finite, $\Lambda = k$, then this is just R^k.

Definition 1.69. Our **standard basis** in R^k is

$$e_1 = (1, 0, ..., 0),$$

$$e_k = (0, ..., 0, 1).$$

Definition 1.70. The **rank** of the free module is k.

In $F = \oplus_{\alpha\in\Lambda} R$, the standard basis is $e_\alpha = (a_\beta)_{\beta\in\Lambda}, a_\alpha = 1, a_\beta = 0$ for $\beta \neq \alpha$.

Definition 1.71. For any $u \in F$, $u = \sum_{\alpha\in\Lambda} a_\alpha e_\alpha$, $a_\alpha \in R$ uniquely, where $a_\alpha = 0$ for all but finitely many α. (Namely, $u = (a_\alpha)_{\alpha\in\Lambda}$).

Remark 1.72. For a basis the representation must be unique, for generators, it does not.

Definition 1.73. Also, if $M \cong F$ for some Λ, M is called **free of rank** $|\Lambda|$.

REMARK 1.74. M is free if and only if it has a basis: a set$\{u_\alpha, \alpha \in \Lambda\} \subseteq M$ s.t. every u in M is uniquely representable in the form:

$$u = \sum_{\alpha \in \Lambda} a_\alpha u_\alpha,$$

where the a's are zero for all but finitely many of them.

DEFINITION 1.75. A set $\{u_\alpha, \alpha \in \Lambda\}$ in a module M is **linearly independent** if $\sum_{\alpha \in \Lambda} a_\alpha u_\alpha = 0$ only if $a_{\alpha_i} = 0$ for all i. In other words, a linear combination is zero if and only if all the coefficients are zero.

REMARK 1.76. A set $\{u_\alpha, \alpha \in \Lambda\}$ is a basis in M if and only if it is linearly independent and generates M. (It is unique since if we have two representations $u = \sum_{\alpha \in \Lambda} a_\alpha u_\alpha = \sum_{\alpha \in \Lambda} b_\alpha u_\alpha$, then $\sum_{\alpha \in \Lambda}(a_\alpha - b_\alpha)u_\alpha = 0$ so by linear independence, all the differences of coefficients are zero.)

THEOREM 1.77. *Any vector space is a free module. More generally, if R is a division ring, the any R module is free.*

PROOF. Let M be a nonzero R-module. Take the maximum linearly independent set B in M. It exists by Zorn Lemma. Indeed, take a nonzero element $u \in M$, then $\{u\}$ is linearly independent (proof is elementary, requires that R is a division ring). If you have a chain/subset tower of linearly independent sets, then their union is linearly independent, by Zorn Lemma. If $\mathcal{B}$ is a chain of linearly independent sets in M, the n $\bigcup \mathcal{B}$ is linearly independent. If

$$u_1, ..., u_n \in \bigcup \mathcal{B},$$

$$\sum_{i=1}^{n} a_i u_i = 0,$$

find $C \in \mathcal{B}$ s.t. these u's are all in C, C is linearly independent, so $a_i = 0$ for all i. So Zorn applies, and B exists. Now we claim that B generates M so B is a basis by Remark 10.76.

PROOF. Let $u \notin RB$. Then $B \cup \{u\}$ is linearly independent, contradiction, since then it would be bigger than B but B is maximal. Indeed, if:

$$au + \sum_{i=1}^{k} a_i u_i = 0,$$

for some $u_{\alpha_i} \in B$ for all i. If $a = 0$, then all a's are zero, since B is linearly independent. If a is note zero, then $u = -a^{-1} \sum_{i=1}^{k} a_i u_i \in RB$, which is impossible, since we said $u \notin RB$ at beginning of claim. □

□

REMARK 1.78. It is impossible for all of M to be linearly independent since we have u and $2u$ which are clearly dependent.

EXAMPLE 1.79. $\mathbb{R}$ is a vector space over $\mathbb{Q}$. We need Hamel basis. We start with $\{1, \alpha_1, \alpha_2, ...\}$, you need to get more than countably many. This has something to do with Zorn Lemma. The process cannot be defined with an algorithm.

DEFINITION 1.80. The rank of a vector space is called the **dimension**.

THEOREM 1.81. *The dimension of a vector space is uniquely defined: If R is a field, or a division ring, then $R^n \ncong R^m$ for $n \neq m$. This is for finite dimension, but for infinite dimensions it is also true.*

PROOF. **Finite Case:** Let R be a division ring, let M be an R-module, let $\{u_1, ..., u_n\}$, and $\{v_1, ..., v_m\}$ be two bases in M. We claim $m = n$.

PROOF. Assume that $n \geqslant m$. We have $v_1 = a_1u_1 + \cdots a_nu_n$ for some coefficients not all zero. Without loss of generality, assume that the first a_1 is nonzero. Then:

$$u_1 = a_1^{-1}v_1 - a_1^{-1}a_2u_2 - \cdots - a_1^{-1}a_nu_n.$$

Then $R\{v_1, u_2, ..., u_m\} = M$: if

$$v = \sum_{i=1}^{n} b_iu_i = b_1u_1 + \sum_{i=2}^{n} b_iu_i = b_1(a_1^{-1}v_1 - a_1^{-1}a_2u_2 - \cdots) + \sum b_iu_i = cv_1 + \sum_{i=2}^{n} c_i = u_i.$$

And $\{v_1, u_2, ..., u_n\}$ is linearly independent: if

$$cv_1 + c_2u_2 + \cdots + c_nu_n = 0 = c(a_1u_1 + \cdots a_nu_n) + c_2u_2 + \cdots + c_nu_n = ca_1u_1 + \sum i = 2^n d_iu_i,$$

then $ca_1 = 0$, so $c = 0$, so all c's are zero. Hence $\{v_1, u_2, ..., u_n\}$ is a basis. Next, replace one of $u_2, ..., u_n$ by v_2, and without loss of generality, replace u_2 with v_2. And after m steps, we see that $\{v_1, ..., v_m, u_{m+1}, ..., u_n\}$ is a basis. But $\{v_1, ..., v_m\}$ is a basis, so by definition those extra u's don't exist, and $n = m$. □

REMARK 1.82. If R is commutative and unital, then the rank of a free R-module is well defined:

$$R^n \ncong R^m,$$

where $n \neq m$.

PROOF. Let I be a maximal ideal in R, exists by Zorn Lemma. The R/I is a field. Then $R^n/(IR^n) \cong (R/I)^n = F^n$, where R^n is the free module of rank n. And $R^m/(IR^m) \cong F^m$. And $F^n \ncong F^m$ since dimension is well defined, so $R^n \ncong R^m$. □

□

Friday, January 19th We do exercises from Section 10.2,3.

DEFINITION 1.83. An R-module is called a **torsion module** if for each $m \in M$, there exists a nonzero $r \in R$ s.t. $rm = 0$.

Monday, January 22th

REMARK 1.84. Any module M has a maximal linearly independent set B of elements, by Zorn Lemma.

LEMMA 1.85. *If M is a torsion module, this set is empty.*

PROOF. Any element is not linearly independent if you take it alone. $\forall u\ \exists a \neq 0$, s.t. $au = 0$. □

However, B doesn't have to generate M. So what can we say about the submodule generated by B. The submodule RB has as basis (B), a linearly independent system which generates this module. **So, it's free.** And in fact:

REMARK 1.86. It is the maximal free submodule: when you factorize by this submodule, you get a torsion ring.

LEMMA 1.87. *M/RB is a torsion module if and only if B is a **maximal linearly independent set**.*

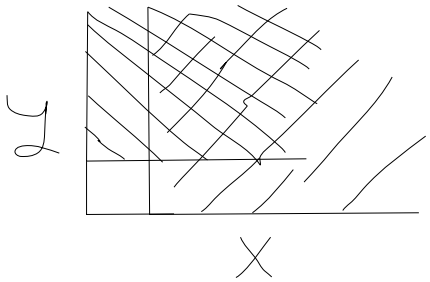
PROOF. We assume R is unital, since otherwise, B may not be in RB. Or we could define RB as $RB \cup B$. Indeed, if $\exists u \in M$ s.t. $\overline{u} \equiv u \mod RB$ is not a torsion element, this means that $au \notin RB \ \forall a \neq 0 \in R$. This is because "0" in the quotient module is the kernel, RB so au cannot be in RB. Then if:

$$au + c_1 v_1 = \cdots c_k v_k = 0,$$

with $v_i \in B, c_i \in R, a \in R$, then $a = 0$, since if a was nonzero, then $au = -c_1 v_1 - \cdots - c_k v_k \in RB$. so $c_1 v_1 + \cdots c_k v_k = 0$, so $c_i = 0$ for all i, so $\{u\} \cup B$ is linearly independent, contradiction, since B was the largest linearly independent set in M.

For any u, there exists a nonzero a s.t. $a\overline{u} \in RB$, so $au + c_1 v_1 + \cdots c_k v_k = 0$ for some $c_i \in R, v_i \in B$. □

EXAMPLE 1.88. Let $R = F[x, y], M = (x, y)$. The lines represent the ideals $(x), (y)$, and the empty box in the bottom left corner are just the constants.



$B = \{ x \}$. $RB = (x)$. And $M/RB = M/(x)$.

10.3 Exercises

7. *Let N be a submodule of M. Prove that if both M/N and N are finitely generated, then so is M.*

   PROOF. Suppose M is not finitely generated. Then we have:

   $$M/N = RA,$$

   where $A = \{x_1 + N, ..., x_n + N\}$. And since N is also finitely generated, we know $N = RA_N$, and $M - N$ is not finitely generated. Now we know $x_i \in M - N$ since otherwise we would have $x_i + N = N$. So then since M is not finitely generated, we know $\exists y \in M - N$ s.t. $y \notin R\{x_i\}$, hence $y + N \notin RA = \{(rx_1) + N, ..., (rx_n) + N\}$, but since $y \in M - N$ we know $y + N \neq N$, hence $y + N \in M/N$. But we said $M/N = RA$, so this is a contradiction, so we must have that M is finitely generated. □

12. *Let R be a commutative ring and let A, B, and M be R-modules. Prove the following isomorphisms of R-modules:*

(a) $Hom_R(A \times B, M) \cong Hom_R(A, M) \times Hom_R(B, M)$.

PROOF. Let $H = \mathrm{Hom}_R(A \times B, M)$, $H_A = \mathrm{Hom}_R(A, M)$, and $H_B = \mathrm{Hom}_R(B, M)$. Let $\Phi : H_A \times H_B \to H$ be given by $\Phi((\varphi, \psi)) = \varphi + \psi$, where $\varphi \in H_A, \psi \in H_B$. We prove this is an isomorphism of R-modules.

Homomorphism: Observe:

$$\begin{aligned}\Phi((\varphi_1, \psi_1) + (\varphi_2, \psi_2)) &= \Phi((\varphi_1 + \varphi_2, \psi_1 + \psi_2)) = \varphi_1 + \psi_1 + \varphi_2 + \psi_2 \\ &= \Phi((\varphi_1, \psi_1)) + \Phi((\varphi_2, \psi_2)).\end{aligned} \tag{1.6}$$

In the above expression, the first equality comes from the definition of addition in $H_A \times H_B$. The second and third equalities comes from the definition of Φ. And we also know:

$$\Phi(r(\varphi, \psi)) = \Phi((r\varphi, r\psi)) = r\varphi + r\psi = r(\varphi + \psi) = r\Phi((\varphi, \psi)),$$

hence Φ preserves mult. by R, by the definition of scalar multiplication on the R-module $H_A \times H_B$, and the definition of Φ.

Surjectivity: Let $\varphi \in H$. Then $\varphi : A \times B \to M$. So let $\varphi \in H_A$ be given by $\varphi(a) = \varphi(a, 0)$, and let $\psi \in H_B$ be given by $\varphi(b) = \varphi(0, b)$. Then we have: $\Phi((\varphi, \psi)) = \varphi$. Then Φ is surjective.

Injectivity: Let $\Phi((\varphi_1, \psi_1)) = \varphi_1 + \psi_1 = \varphi_2 + \psi_2 = \Phi((\varphi_2, \psi_2)) \in H_A \times H_B$. Then note that

$$(\varphi_1 + \psi_1)(a, 0) = \varphi_1(a) = \varphi_2(a) = (\varphi_2 + \psi_2)(a, 0),$$

and the same holds when we let $a = 0$, and use an arbitrary b value, so we get that $\psi_1 = \psi_2$ as well. Hence Φ is injective. And thus it is an isomorphism. □

(b) $Hom_R(M, A \times B) \cong Hom_R(M, A) \times Hom_R(M, B)$.

PROOF. Let $H = \mathrm{Hom}_R(M, A \times B)$, $H_A = \mathrm{Hom}_R(M, A)$, and $H_B = \mathrm{Hom}_R(M, B)$. Let $\Phi : H_A \times H_B \to H$ be given by $\Phi((\varphi, \psi)) = (\varphi, \psi) \in H$, where $\varphi \in H_A$, and $\psi \in H_B$. We prove this map is an isomorphism.

Homormorphism: Observe:

$$\begin{aligned}\Phi((\varphi_1, \psi_1) + (\varphi_2, \psi_2)) &= \Phi((\varphi_1 + \varphi_2, \psi_1 + \psi_2)) = (\varphi_1 + \varphi_2, \psi_1 + \psi_2) \\ &= (\varphi_1, \psi_1) + (\varphi_2, \psi_2) = \Phi((\varphi_1, \psi_1)) + \Phi((\varphi_2, \psi_2)).\end{aligned} \tag{1.7}$$

The first equality follows from addition in the R-module $H_A \times H_B$, the second comes from the definition of Φ, the third comes from addition in H, and the last again comes from the definition of Φ. And we also know:

$$\Phi(r(\varphi, \psi)) = \Phi((r\varphi, r\psi)) = (r\varphi, r\psi) = r(\varphi, \psi) = r\Phi((\varphi, \psi)),$$

by the definition of scalar mult. in H, hence since Φ preserves addition and scalar multiplication, we know it is a homomorphism.

Surjectivity: Let $\varphi \in H$, then we know $\varphi : M \to A \times B$. Then the image of any element of M under φ is a two dimensional vector whose first component lives in A, and whose second component lives in B. So let $\varphi : M \to A$ be given by $\varphi(m) = \varphi(m)_1$, the first component of $\varphi(m)$. and let $\psi(m) = \varphi(m)_2$. Then $\Phi((\varphi, \psi)) = (\varphi, \psi) = \varphi$. Hence Φ is surjective.

Injectivity: Let $\Phi((\varphi_1, \psi_1)) = (\varphi_1, \psi_1) = (\varphi_2, \psi_2) = \Phi((\varphi_2, \psi_2))$. Then we must have $\varphi_1 = \varphi_2$, and $\psi_1 = \psi_2$, since otherwise we do not have equality of these ordered pairs of hom-sms in H. But then we have shown that the arguments of Φ are equal in this case, so Φ must be injective. □

15. *An element $e \in R$ is called a **central idempotent** if $e^2 = e$ and $er = re$ for all $r \in R$. If e is a central idempotent in R, prove that $M = eM \oplus (1-e)M$.*

PROOF. So we wish to show that M is the direct sum of the two specified submodules. Note that we know that these sets are both submodules by Exercise 14 of Section 1, which tells us that zM is a submodule for any z in the center of R. We know e is in the center since it is a central idempotent. And $(1-e)r = r - er = r - re = r(1-e)$. So it is also in the center. Now we need only show that $M = eM + (1-e)M$, and that $eM \cap (1-e)M = 0$.

Let $m \in M$. Then $m = em + (1-e)m = em + m - em$, where $em \in eM$, and $(1-e)m \in (1-e)M$, so $m \in eM + (1-e)M$. Now let $em + (1-e)n \in eM + (1-e)M$. Then we have $em + n - en = n + e(m-n)$. So we know $M = eM + (1-e)M$. So let $m \in eM \cap (1-e)M$. Then $m = en_1 = (1-e)n_2$ for some $n_1, n_2 \in M$. Then we have:

$$m = en_1 = (1-e)n_2 = e^2 n_1 = e(1-e)n_2 = (e-e^2)n_2 = (e-e)n_2 = 0,$$

so we have shown that if $m \in eM \cap (1-e)M$, $m = 0$, so $eM \cap (1-e)M = 0$. And thus $M = eM \oplus (1-e)M$ by definition. □

18. *Let R be a PID, let M be an R-module, and assume that $aM = 0$ for some $a \neq 0$ where $a \in R$. Let:*

$$a = p_1^{r_1} \cdots p_k^{r_k},$$

distinct primes in R $\forall i$, and let:

$$M_i = Ann(p_i^{r_i}) = \{u \in M : p_i^{r_i} u = 0\}.$$

Then $M = M_1 \oplus \cdots \oplus M_k$.

PROOF. $\forall i$, let $a_i = a/p_i^{r_i} (= \prod_{j \neq i} p_j^{r_j})$. Then $a_i M \subseteq M_i$, since $p_i^{r_i}(a_i M) = aM = 0$ (by assumptions of theorem). Then:

$$gcd(a_1, ..., a_k) = 1,$$

so there exists $c_1, ..., c_k \in R$ s.t. $c_1 a_1 + \cdots + c_k a_k = 1$. So $\forall u \in M$,

$$u = c_1 a_1 u + \cdots + c_k a_k u \in M_1 + \cdots M_k.$$

Now let $u \in M_i \cap (\sum_{j \neq i} M_j)$. Then $p_i^{r_i}, a_i \in Ann(u)$. So, $(p_i^{r_i}) = (1) \subseteq Ann(u)$, so $u = 0$. So $\forall i, M_i \cap (\sum_{j \neq i} M_j) = 0$. □

22. *Let R be a Principal Ideal Domain, let M be a torsion R-module, and let p be a prime in R (do not assume M is finitely generated, hence it need not have a nonzero annihilator). The **p-primary component of** M is the set of all elements of M that are annihilated by some positive power of p.*

(a) *Prove that the p-primary component is a submodule.*

PROOF. Let N denote the p-primary component of M. Note that:

$$N = \left\{ m \in M : \exists k \in \mathbb{N}, p^k m = 0 \right\}.$$

We apply the submodule criterion. Note that $N \neq \varnothing$ since $0 \in N$. Let $x, y \in N$, and let $r \in R$. Then we know $\exists k, l \in \mathbb{N}$ s.t. $p^k x = p^l y = 0$. Observe:

$$p^k p^l (x + ry) = p^l p^k x + r p^k p^l y = p^l 0 + r p^k 0 = 0,$$

so we know $x + ry \in N$, hence by the submodule criterion, N is a submodule of M. □

(b) *Prove that this definition of p-primary component agrees with the one given in Exercise 18 when M has a nonzero annihilator.*

PROOF. Assume M has a nonzero annihilator a, and this is the minimal such element. Then let p^α be a prime power factor in the prime factorization of a. Let:

$$N = \left\{ \, m \in M : \exists k \in \mathbb{N}, p^k m = 0 \, \right\}.$$

In Exercise 18, the definition given for the annihilator of p^α is:

$$A = Ann_M(p^\alpha) = \{m \in M : p^\alpha m = 0\}.$$

So clearly any element of A is in N; just let $k = \alpha$. So let $m \in N$. Then $\exists k \in \mathbb{N}$ s.t. $p^k m = 0$. Suppose $k > \alpha$. Then since $am = 0$, we must have some other product of primes $r = r_1 \cdots r_l \mid a$ s.t. $r \nmid p^\alpha$. But since we proved that N is a submodule in part (a), we know $Ann(N) = \{ \, r \in R : rm = 0, \forall m \in N \, \}$ is an ideal in R. Note then that $r, p^k \in Ann(N)$. But since $p^k \nmid r$ since otherwise we would have $p^k \mid a$, which is impossible since we said $r > \alpha$. So then $r \notin Rp^k$, hence $Ann(N)$ is not a principal ideal, but this is impossible, since we are in a PID, so we must have $k \leqslant \alpha$. Hence $m \in A$, and thus $N \subseteq A$, and the definitions are equivalent, because the sets are equal.

□

(c) *Prove that M is the (possibly infinite) direct sum of its p-primary components $\{ \, M_i \, \}$, as p runs over all primes of R.*

PROOF. Let $\{ \, p_i \, \}$ be all the primes in R. $\forall i$, let $a_i = \prod_{j \neq i} p_j^{r_j}$. Then $a_i M \subseteq M_i$, since $p_i^{r_i}(a_i M) = \prod_{j=1}^{\infty} p_j^{r_j} M = 0$ (since M is a torsion module, and hence $\forall m \in M$ there exists a nonzero $r \in R$ s.t. $rm = 0$, and the prime decomposition of r is in $\prod_{j=1}^{\infty} p_j^{r_j}$). Then:

$$gcd(a_1, a_2, ...) = 1,$$

so there exists $c_1, c_2, ... \in R$ not necessarily all nonzero s.t. $c_1 a_1 + \cdots = 1$. So $\forall u \in M$,

$$u = \sum_{i=1}^{\infty} c_i a_i \in M_1 + M_2 + \cdots .$$

Now let $u \in M_i \cap (\sum_{j \neq i} M_j)$. Then $p_i^{r_i}, a_i \in Ann(u)$. So, $(p_i^{r_i}) = (1) \subseteq Ann(u)$, so $u = 0$. So $\forall i, M_i \cap (\sum_{j \neq i} M_j) = 0$. So since we know $M = M_1 + M_2 + \cdots$, and the pairwise intersection of each of these is 0, we know that $M = M_1 \oplus M_2 \oplus \cdots$. □

27. *We show that* ***free modules over noncommutative rings need not have a unique rank.*** *Let $M = \mathbb{Z}^{\mathbb{N}} = \{ \, (a_1, ..., a_n) : a_i \in \mathbb{Z} \, \}$. Let $R = End_{\mathbb{Z}}(M)$. Consider R as a module over itself. It is a free module of rank 1. We claim $R \cong R^2$. And so we would have $R \cong R^n$ for any n.*

PROOF. Consider $\varphi_1, \varphi_2, \psi_1, \psi_2 \in R$. Define:

$$\begin{aligned} \varphi_1(a_1, a_2, ...) &= (a_1, a_3, a_5, ...) \\ \varphi_2(.....) &= (a_2, a_4, ...) \\ \psi_1(.....) &= (a_1, 0, a_2, 0, ...) \\ \psi_2(.....) &= (0, a_1, 0, a_2, ...) \end{aligned} \tag{1.8}$$

We claim that $\{ \varphi_1, \varphi_2 \}$ is a basis of R as an R-module, so $R \cong R^2$ as R-modules. **Why this implication!! Ask after class.** The general situation: M is R module, $u_1, ..., u_n$ is basis in M. Then every element of M is a linear combination uniquely. Then $M \cong R^n$ under isomorphism $u \mapsto (a_1, ..., a_n)$, the coefficients of the unique linear combination representing u. We have:

$$\varphi_1\psi_1 = \varphi_2\psi_2 = 1,$$

$$\varphi_1\psi_2 = \varphi_2\psi_1 = 0,$$

$$\psi_1\varphi_1 + \psi_2\varphi_2 = 1.$$

These can be checked easily. Any $\varphi = \varphi 1 = (\varphi\psi_1)\varphi_1 + (\varphi\psi_2)\varphi_2)$. So φ_1, φ_2 generate φ. If $\beta_1\varphi_1 + \beta_2\varphi_2 = 0$, then $\beta_1\varphi_1\psi_1 + \beta_2\varphi_2\psi_1 = 0$. So we get $\beta_1 = 0$. And to get $\beta_2 = 0$, we multiply on the right by ψ_2 instead of ψ_1. And they are linearly independent. And thus a basis, so the claim is fulfilled. □

0. *Let M be an R-module and let I, J be ideals in R.*
   (a) *Prove that $Ann(I + J) = Ann(I) \cap Ann(J)$.*
   PROOF. Let $m \in Ann(I + J)$. Then $(i + j)m = 0$ for all $i \in I, j \in J$. Then letting $i = 0$, we know $m \in Ann(J)$, and letting $j = 0$, we know $m \in Ann(I)$. So $Ann(I + J) \subseteq Ann(I) \cap Ann(J)$. Now let $m \in Ann(I) \cap Ann(J)$. Then $im = 0, \forall i \in I$, and $jm = 0, \forall j \in J$. Then we have:
   $$(i + j)m = im + jm = 0 + 0 = 0,$$
   by he definition of an R-module. So $Ann(I) \cap Ann(J) \subseteq Ann(I + J)$. Hence they are equal. □
   (b) *Prove that $Ann(I) + Ann(J) \subseteq Ann(I \cap J)$.*
   PROOF. Let $m \in Ann(I) + Ann(J)$. Then $m = n + k$ for some $n \in Ann(I), k \in Ann(J)$. Let $i \in I \cap J$. Then we know:
   $$im = i(n + k) = in + ik = 0 + 0 = 0,$$
   by the distributivity of the action of R on M, and since $i \in I$, and $i \in J$, and since n, k are in the respective annihilators. Thus $m \in Ann(I \cap J) \Rightarrow Ann(I) + Ann(J) \subseteq Ann(I \cap J)$. □
   (c) *Give an example where the inclusion in part (b) is strict.*
   Let R be the ring of continuous functions $f : [0, 1] \to \mathbb{R}$. Note this is not an integral domain since we can construct zero divisors in the form of a pair piecewise functions, one of which is zero on half the interval, and the other being zero on the other half. We consider the R-module of R over itself. Then let I be the ideal of functions which are zero on $[0, 1/2]$, and J be the ideal of functions which are zero on $[1/2, 1]$. Now note that $I + J \neq R$ since $f(x) = 1$ is in R, but not in $I + J$, since all functions in $I + J$ are zero at $1/2$. But $I \cap J = 0$,

since these functions must be zero across both halves, and so $Ann(I \cap J) = R$, and so $Ann(J) + Ann(I) = I + J \subsetneq R = Ann(I \cap J)$.
We give another example. Consider $R = F[x, y]$,

$$M = R/(xy) = \{ a_0 + b_1 x + \cdots b_n x^n + c_1 y + \cdots + c_n y^n \}.$$

$I = (x), J = (y)$, and $I \cap J = (xy)$. Then we have:

$$\begin{aligned} Ann(I) &= \{ c_1 y + \cdots + c_n y^n \} \subseteq M, \\ Ann(J) &= \{ b_1 x + \cdots + b_n x^n \}. \end{aligned} \tag{1.9}$$

And $Ann(I \cap J) = Ann(xy) = M$. And $F \subseteq Ann(I \cap J) \subsetneq Ann(I) + Ann(J)$.

(d) *If R is commutative and unital and I, J are comaximal, prove that $Ann(I \cap J) = Ann(I) + Ann(J)$.*

Proof. Assume R is commutative and unital, and I, J are comaximal. Let $m \in Ann(I + J) = Ann((1)) = Ann(R)$ since I, J are comaximal, and R is commutative and unital. So $rm = 0$ for all $r \in R$. So then $m \in Ann(I)$, and since $0 \in Ann(J)$, we may write $m = m + 0$, so $m \in Ann(I) + Ann(J)$. And thus $Ann(I + J) \subseteq Ann(I) + Ann(J)$. So they are equal by the result of part (b). **This is just very wrong, I think.** □

1.4. Tensor Products of Modules

Monday, January, 22nd
Let R be a unital, commutative ring. Let M, N be R-modules. We have:

$$M \times N = M \oplus N.$$

i.e. $(u, v) = u + v = (u, 0) + (0, v)$. If we want to actually multiply M, N, multiply elements of M and elements of N: uv. Then the first thing we need is for it to be distributive. Then we want:

$$\begin{aligned} (u_1 + u_2)v &= u_1 v + u_2 v, \\ u(v_1 + v_2) &= uv_1 + uv_2. \end{aligned} \tag{1.10}$$

Definition 1.89. A mapping $\beta : M \times N \to K$ is said to be **bilinear** if for all $v \in N$, $\beta : (\cdot, v) : M \to K$ is a hom-sm, and for any $u \in M$, $\beta(u, \cdot) : N \to K$ is a hom-sm, that is, $\forall v \in N, \forall u_1, u_2 \in M$:

$$\beta(u_1 + u_2, v) = \beta(u_1, v) + \beta(u_2, v).$$

And $\forall u \in M, a \in R$:

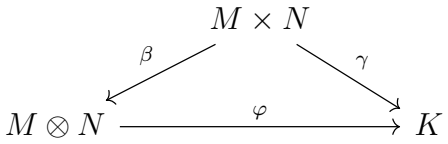
$$\beta(au, v) = a\beta(u, v).$$

And $\forall u \in M, \forall v_1, v_2 \in N$:

$$\beta(u, v_1 + v_2) = \beta(u, v_1) + \beta(u, v_2).$$

Where above, we put $\beta_v(u) = \beta(u, v)$ for all $u \in M$. $\beta_v : M \to K$.

Definition 1.90. The **tensor product** $M \otimes_R N$ is an R-module with a bilinear mapping $\beta : M \times N \to M \otimes N$ such that for any module K, and any bilinear mapping $\gamma : M \times N \to K$, there is a unique homomorphism $\varphi : M \otimes N \to K$ such that $\gamma = \varphi \circ \beta$, i.e.:



is commutative.

In the above diagram, the top and left nodes together are the universal object. And the morphism is φ.

We need to prove this because the above definition is not constructive. We just said it's a module with certain properties. Now we construct it explicitly. If such a module exists, then it is unique up to isomorphism.

PROPOSITION 1.91. *$M \otimes N$ exists.*

PROOF. Let $\mathcal{M}$ be the free R-module generated by $M \times N$ - as a set. That is, the set of formal linear combinations of pairs $(u, v) \in M \times N$. So:

$$\mathcal{M} = \{\, a_1(u_1, v_1) + \cdots + a_n(u_n, v_n) : a_i \in R, (u_i, v_i) \in M \times N \,\}.$$

Let $\mathcal{L}$ be the submodule of $\mathcal{M}$ generated by elements of the form:

$$\begin{aligned} (u_1 + u_2, v) - (u_1, v) - (u_2, v), \\ (u, v_1 + v_2) - (u, v_1) - (u, v_2), \\ (au, v) - a(u, v), \\ (u, av) - (a(u, v)). \end{aligned} \tag{1.11}$$

We want the bilinearity relations to be satisfied, so we declare all these elements to be zero. Claim: $\mathcal{M}/\mathcal{L} = M \otimes N$. So what are elements of this module? These are classes of linear combinations of pairs. Elements of $\mathcal{M}/\mathcal{L}$ are classes (module $\mathcal{L}$) of linear combinations of (u, v). The class of (u, v) is denoted by $u \otimes b$. So

$$\mathcal{M}/\mathcal{L} = \left\{ \sum a_i(u_i \otimes v_i) : a_i \in R, u_i \in M, v_i \in N \right\}.$$

DEFINITION 1.92. The elements of of the set above are called **tensors**, and $u \otimes v$ is called a **simple tensor**.

So:

$$\mathcal{M}/\mathcal{L} = \left\{ \sum a_i \overline{(u_i, v_i)} \right\}.$$

And:

$$\begin{aligned} \overline{(u, v)} &= u \otimes v, \\ \overline{(u_1 + u_2, v)} &= \overline{(u_1, v)} + \overline{(u_2, v)}, \\ (u_1 + u_2) \otimes v &= u_1 \otimes v + u_2 \otimes v. \end{aligned} \tag{1.12}$$

The mapping $M \times N \to \mathcal{M}/\mathcal{L}$ given by $(u, v) \mapsto u \otimes v$ is bilinear: in $\mathcal{M}/\mathcal{L}$, we have:

$$\begin{aligned} (u_1 + u_2) \otimes v &= u_1 \otimes v + u_2 \otimes v, \\ \beta(u_1 + u_2, v) &= \beta(u_1, v) + \beta(u_2, v), \end{aligned} \tag{1.13}$$

where the stuff in the bottom line is equal to the stuff it lines up with in the top line. Also:

$$\begin{aligned}(au)\otimes v &= a(u\otimes v),\\ u\otimes(v_1+v_2) &= u\otimes v_1 + u\otimes v_2,\\ u\otimes(av) &= a(u\otimes v).\end{aligned} \tag{1.14}$$

if $\gamma : M\times N\to K$ is bilinear, we have a unique homomorphism $\Phi : M\to K$ with $\Phi(u,v) = \gamma(u,v)$ for all u, v.

Since γ is bilinear, $\Phi(\mathcal{L}) = 0$,

$$\begin{aligned}(\Phi(u_1+u_2,v)-(u_1,v)-(u_2,v)) &= \Phi(u_1+u_2,v)-\Phi(u_1,v)-\Phi(u_2,v)\\ &= \gamma(u_1+u_2,v)-\gamma(u_1,v)-\gamma(u_2,v).\end{aligned} \tag{1.15}$$

and the same holds for all other relations. So Φ is factorized to a hom-sm $\varphi : \mathcal{M}/\mathcal{K}\to K$. It is unique since $\mathcal{M}$ is generated by $M\times N$ s.t. $\varphi(u\otimes v) = \gamma(u,v)$. □

Tuesday, January 23rd

Let R be commutative, unital. And M, N be R-modules. Then: $M\otimes N = M\otimes_R N$ is an R-module consisting of **tensors:**

$$a_1(u_1\otimes v_1)+\cdots+a_n(u_n\otimes v_n),$$

with $a_i\in R, u_i\in M, v_i\in N$. It is generated by **simple tensors** $u\otimes v$, with relations:

$$\begin{aligned}(u_1+u_2)\otimes v &= u_1\otimes v + u_2\otimes v,\\ (au)\otimes v &= a(u\otimes v),\\ u\otimes(v_1+v_2) &= u\otimes v_1+u\otimes v_2,\\ u\otimes(av) &= a(u\otimes v).\end{aligned} \tag{1.16}$$

And it has no other relations! It has a universal property: for any R-module K and a bilinear mapping $\gamma : M\times N\to K$ there exists a unique hom-sm $\varphi : M\otimes N\to K$ such that $\varphi(u\otimes v) = \gamma(u,v)$ for each $u\in M, v\in N$.

Lemma 1.93. *We list some properties.*

(1) If $M = RB$, $N = RC$, then $M\otimes N = R(B\otimes C)$, where $B\otimes C = \{\, u\otimes v : u\in B, v\in C\,\}$.

Proof. $\forall u\in M$, $u = \sum a_iu_i, u_i\in B$. And $\forall v\in N, v = \sum b_jv_j, v_j\in C$. Then:

$$u\otimes v = \sum_{i,j} a_ib_j(u_i\otimes v_j).$$

i.e. any tensor in $M\otimes N$ is a linear combinations of such simple tensors. □

(2) $\forall u\in M$, $u\otimes 0 = 0$, and $\forall v\in N$, $0\otimes v = 0$.

Proof. $u\otimes 0 = u\otimes(0+0) = u\otimes 0+u\otimes 0$, so we must have that it is zero. □

(3) $\forall$ module M, $M\otimes 0 = 0\otimes M = 0$.

(4) $\forall$ module M, $M\otimes R\cong R\otimes M\cong M$.

R plays the role of the identity in this algebra of modules.

PROOF. Take any tensor, it is of the form:

$$\begin{aligned} a_1(u_1 \otimes b_1) + \cdots + a_n(u_n \otimes b_n) &= a_1b_1(u_1 \otimes 1) + \cdots + a_nb_n(u_n \otimes 1) \\ &= (a_1b_1u_1) \otimes 1 + \cdots + (a_nb_nu_n) \otimes 1 \\ &= (a_1b_1u_1 + \cdots + a_nb_nu_n) \otimes 1 = v \otimes 1. \end{aligned} \tag{1.17}$$

Note in the above, $b_i \in R$, so we can take them out: $u \otimes b = u \otimes (b \cdot 1) = b(u \otimes 1)$.

So define a hom-sm $\varphi : M \otimes R \to M$ by:

$$\sum_{i=1}^{n} b_i(u_i \otimes a_i) \mapsto \sum_{i=1}^{n} a_ib_iu_i.$$

Why is φ defined, and why is it a homomorphism? First, define $\gamma : M \times R \to M$, $\gamma(u, a) = au$. This γ is bilinear. If u is fixed, it is linear with respect to a, if a is fixed, it is linear with respect to u. So there exists a unique hom-sm $\varphi : M \otimes R$ s.t. $\varphi(u \otimes a) = au \ \forall u \in M, a \in R$. This is our φ. Why is it an isomorphism. Construct the inverse mapping. Take $u \mapsto u \otimes 1$. And why do we need to prove that it is defined? There are relations in the module.

EXAMPLE 1.94. The same tensor can be written in several ways as a sum of simple tensors, in $\mathbb{Z} \otimes \mathbb{Z}$:

$$5 \otimes 6 = 2 \otimes 6 + 3 \otimes 6.$$

The left hand side is sent to 30, but we need it to be bilinear or something.

So the inverse is a homomorphism, $M \to M \otimes R$. It is an inverse, since if we start with a tensor, send it to the $v \otimes 1$ in Equation 1.17, we get:

$$\sum a_i(u_i \otimes b_i) \mapsto^{\varphi} \sum a_ib_iu_i \mapsto^{\varphi^{-1}} (\sum a_ib_iu_i) \otimes 1.$$

□

(5) *$M \otimes N \cong N \otimes M$ by the map $u \otimes v \mapsto v \otimes u$. We send $(u, v) \mapsto v \otimes u$ - linear, so φ exists. And $v \otimes u \mapsto u \otimes v$ is its inverse.*

(6) *$M \otimes N) \otimes K \cong M \otimes (N \otimes K)$ by the map:*

$$(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w).$$

(7) *$M \otimes (M \oplus K) \cong (M \otimes K) \oplus (M \otimes K)$.*

So in naive set theory, any collection of objects is a set, but this leads to immediate crap. So we use ZFC, axiomatic. Modules don't form a set because there are too many of them, lmao.

PROOF. Let $\varphi : u \otimes (v, w) \mapsto (u \otimes v, u \otimes w)$. We only define φ on simple tensors, then by linearity, it is extended to all tensors. Is it well defined? Yes, φ is a well-defined hom-sm if:

$$(u, (v, w)) \mapsto (u \otimes v, u \otimes w),$$

is bilinear. The stuff on the left side, domain, is in $M \times (N \oplus K)$. So we check it:

$$\begin{aligned} (u_1 + u_2, (v, w)) \mapsto ((u_1, u_2) \otimes v, (u_1, u_2) \otimes w) &= (u_1 \otimes v + u_2 \otimes v, u_1 \otimes w + u_2 \otimes w) \\ &= (u_1 \otimes v, u_1 \otimes w) + (u_2 \otimes v, u_2 \otimes v). \end{aligned} \tag{1.18}$$

To prove that this is an ismorphism, we need its inverse. Define $\psi : (M \otimes N) \oplus (M \otimes K) \to M \otimes (N \oplus K)$. The direct sum is also a universal object. Define $\psi_1 : M \otimes N \to M \otimes (N \oplus K), \psi_2 : M \otimes K \to M \otimes (N \oplus K)$ by:

$$\begin{aligned} \psi_1(u \otimes v) &= u \otimes (v, 0), \\ \psi_2(u \otimes w) &= u \otimes (0, w). \end{aligned} \tag{1.19}$$

There is a unique hom-sm ψ s.t. $\psi|_{M\otimes N} = \psi_1$, and $\psi|_{M\otimes K} = \psi_2$. So we have:

$$(\psi(\alpha, \beta) = \psi_1(\alpha) + \psi_2(\beta)).$$

So we check that they are inverses of each other. We have:

$$\varphi : u \otimes (v, w) \mapsto (u \otimes v, u \otimes w) \mapsto_\psi u \otimes (v, 0) + u \otimes (0, w) = u \otimes (v, w). \tag{1.20}$$

□

Wednesday, January 24th

Tensors come from physics, from algebra, from topology. Linear transformations, bilinear forms, ... There are many objects that can be interpreted as tensors. In algebra, they can be used to extend scalars.

Example 1.95. It can be shown that:

$$C(x \times y) = \overline{C(x) \otimes C(y)}.$$

For any R-module M, $M \otimes R \cong M$, and $M \otimes (N \oplus K) \cong (M \otimes N) \oplus (M \otimes K)$.

Remark 1.96. $M \otimes R^n \cong M^n = M \oplus \cdots \oplus M$.

Remark 1.97. $R^n \otimes R^m \cong R^{nm}$-free of rank nm.

Example 1.98. (1) *Prove that $M \otimes R/I \cong M/(IM)$. What number is this????*

Proof. The mapping $\gamma : (u, \overline{a}) = a \mod I \mapsto \overline{au} = au \mod (IM)$. This is well-defined, and is bilinear, so it satisfies the properties required for a tensor product. $a + c \mapsto \overline{au + cu} \in IM, c \in I$. So hom-sm $\varphi : M \otimes (R/I) \to M/(IM)$ is defined. And we have: $u \otimes \overline{a} \mapsto \overline{au}$. And it has the inverse: $\psi : \overline{u} \mapsto (u \otimes \overline{1}$, defined from $M/IM \to M \otimes R/I$. You should understand that γ is not an isomorphism itself. Now why is this new map well defined, first? If you replace u by $\overline{u} + \overline{\sum b_i v_i}$, where $b_i \in I$. Then under our new map we have:

$$\psi : \overline{u} = \overline{\sum b_i v_i} \mapsto (u + b_i v_i) \otimes \overline{1} = (u \otimes \overline{1} + \sum (v_i \otimes \overline{b_i},$$

where $\sum (v_i \otimes \overline{b_i} = 0 \mod (M \otimes I)$. So ψ is well-defined, and $\psi = \varphi^{-1}$. □

(2) *Consider $\mathbb{Z}_3 \otimes \mathbb{Z}_2$.*

We may write

$$\begin{aligned} 1 \otimes 1 &= (3 - 2) \otimes 1 \\ &= 3 \otimes 1 - 2 \otimes 1 \\ &= 3 \otimes 1 - 2(1 \otimes 1) \\ &= 3 \otimes 1 - 1 \otimes 2 \\ &= 0 \otimes 1 - 1 \otimes 0 \\ &= 0 - 0 = 0. \end{aligned} \tag{1.21}$$

And for any $n \otimes k = nk(1 \otimes 1) = 0$. So $\mathbb{Z}_3 \otimes \mathbb{Z}_2 = 0$.

LEMMA 1.99. *If $(n, m) = 1$, then $\mathbb{Z}_n \otimes \mathbb{Z}_m = 0$.*

PROOF. There exists k, l s.t. $kn + lm = 1$. Then:

$$1 \otimes 1 = (kn + lm) \otimes 1 = k(n \otimes 1) + l(1 \otimes m) = 0.$$

And $\forall (a \otimes b) = ab(1 \otimes 1) = 0$. □

LEMMA 1.100. *Let $(n, m) = d$. Then $\mathbb{Z}_n \otimes \mathbb{Z}_m \cong \mathbb{Z}_d$.*

PROOF. Define $\varphi : \mathbb{Z}_n \otimes \mathbb{Z}_m \to \mathbb{Z}_d$ by $\varphi(\overline{k} \otimes \overline{l}) = kl \mod d$. If you add a multiple of n to k, the result will be the same because $d|n$, and same for m ($(\overline{k}, \overline{l}) \mapsto kl \mod d$ is bilinear). Why is it a homomorphism? Let's check that it is surjective. Note that $1 \otimes 1 \mapsto 1$, and 1 generates $\mathbb{Z}_d$. So done: $\varphi(1 \otimes a) = a \mod d$, so φ is surjective. Or maybe better to just define an inverse, since injectivity looks hard to prove.

$$\varphi(k(1 \otimes 1)) = k \mod d,$$

for any k, so it's injective or something because the kernel is 0 maybe. □

REMARK 1.101. If G is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1^{r_{1,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{r_{1,k_1}}} \oplus (..p_2..) \oplus \cdots \oplus (..p_l..).$$

So we have $G \otimes_{\mathbb{Z}} \mathbb{Z}_{p_1} \cong \mathbb{Z}{p_1}^{k_1}$. We get this by multiplying by each component and using the previous result, that since the $\mathbb{Z}$'s are relatively prime, they go to zero. So $\forall p \mid |G|$, $G \otimes \mathbb{Z}_p \cong \mathbb{Z}_p^k$ where k is the number of p-elementary divisors of G.

REMARK 1.102. Let R be an integral domain, let F be the field of quotients of R.

$$F \otimes_R M = ?$$

LEMMA 1.103. *If M is a torsion module, then $F \otimes_R M = 0$.*

PROOF. Let $u \in M$. Find $a \neq 0$ s.t. $au = 0$. Then:

$$1 \otimes u = (aa^{-1}) \otimes u = a^{-1} \otimes (au) = 0.$$

But this is not enough. Moreover, for any $b \in F$, we know:

$$b \otimes u = (aa^{-1}b) \otimes u = (a^{-1}b) \otimes (au) = 0.$$

□

EXAMPLE 1.104. Consider $F^2 \otimes F^2 \cong F^4$, where $\{ e_1, e_2 \}$ is a basis. So basis of $F^2 \otimes F^2$ is:

$$\{ e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2 \}.$$

So $F^2 = e_1 F \oplus e_2 F$. Any tensor from $F^2 \otimes F^2$ is of the form:

$$a_{1,1}(e_1 \otimes e_1) + a_{1,2}(e_1 \otimes e_2) + a_{2,1}(e_2 \otimes e_1) + a_{2,2}(e_2 \otimes e_2),$$

its coordinates form:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

So tensors are in bijection with 2×2 matrices. A simple tensor:

$$(a_1 e_1 + a_2 e_2) \otimes (b_1 e_1 + b_2 e_2) \leftrightarrow \begin{pmatrix} a_1 b_1 & a_1 b_2 \\ a_2 b_1 & a_2 b_2 \end{pmatrix},$$

which is degenerate of rank 1. So simple tensors correspond to matrices of rank 1, determinant 0. So note that $(e_1 \otimes e_2) + (e_2 \otimes e_1)$ is not simple.

REMARK 1.105. For an R-algebra S, we have $S \otimes_R$ is an S-module.

Thursday, January 25th

EXAMPLE 1.106. We give an example of when M, N are R-modules but the tensor product of submodules of these are not a submodule of the tensor product of M, N. Note $\mathbb{Z} \subseteq \mathbb{Q}$ as $\mathbb{Z}$-modules. But $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2$, and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2 = 0$.

LEMMA 1.107. *Let S be an R-algebra, M be an R-module then $S \otimes_R M$ has a structure of an S-module by $\alpha(\beta \otimes u) = \alpha\beta \otimes u, \alpha, \beta \in S, u \in M$.*

PROOF. Note we have:

$$\alpha\left(\sum a_i(\beta_i \otimes u_i)\right) = \sum a_i(\alpha\beta_i \otimes u_i). \tag{1.22}$$

The line in the above expression, we are checking if the same thing works for arbitrary tensors, since we defined it in the statement of the problem for just simple tensors. We have to check that elements of the kernel... when we convert the stuff in the left to the right, we have to factorize by a submodule. Is the operation well defined? The operation is: $S \otimes M \to S \otimes M$ where $\beta \otimes u \mapsto \alpha\beta \otimes u$. It is well-defined because it is a bilinear operation: $(\beta, u) \mapsto \alpha\beta \otimes u$. This is our universal approach: first we defined some mapping on simple tensors: $\beta \otimes u \mapsto \alpha\beta \otimes u$, which should be a homomorphism of R-modules. Then to check that it is well-defined, we need to check that it is bilinear on the set $StimesM$. Checking bilinearity:

$$(\alpha\beta, u) \mapsto \alpha a\beta \otimes u = a\alpha\beta \otimes u = a(\alpha\beta \otimes u).$$

Checking conditions, we have:

$$\begin{aligned} (\alpha_1 + \alpha_2)(\beta \otimes u) &= \alpha_1\beta \otimes u + \alpha_2\beta \otimes u = \alpha_1(\beta \otimes u) + \alpha_2(\beta \otimes u), \\ \alpha(w_1 + w_2) &= \alpha w_1 + \alpha w_2, w_i \in S \otimes_R M, \\ \alpha_1(\alpha_2 w) &= (\alpha_1\alpha_2)w. \end{aligned} \tag{1.23}$$

The second line is because $w \mapsto \alpha w$ is a homomorphism. This is called **extension of scalars.** □

EXAMPLE 1.108. We give some examples of **extension of scalars.**

(1) Let F be the field of quotients of an integral domain R. Then $F \otimes_R M$ is an F-module, that is, a vector space. This operation kills all torsion, but preserves the free part. In the case $M = M_1 \oplus M_2$, where M_1 is free, M_2 is torsion. Not always the case, but it is in PID, or in finitely generated abelian groups. So $F \otimes M = F \otimes M \oplus 0$. It has the same rank as M_1. If $M_1 = R^n$, then $F \otimes M_1 \cong F^n$, and it is a vector space.
(2) Let V be an R-vector space. Consider $\mathbb{C} \otimes_{\mathbb{R}} V$ - this is a $\mathbb{C}$-vector space, called **the complexification of V.** We have:

$$\begin{aligned} \mathbb{C} = \mathbb{R} \oplus i\mathbb{R} &= R\{1, i\}, \\ \mathbb{C} \otimes V = (\mathbb{R} \otimes V) \oplus (i\mathbb{R} \otimes V) &= (1 \otimes V) \oplus (i \otimes V). \end{aligned} \tag{1.24}$$

So we have: $a \otimes u = 1 \otimes au$, and $ib \otimes u = i \otimes bu$. So $\forall w \in \mathbb{C} \otimes V$, $w = 1 \otimes u + i \otimes v = u + iv$. Also,

$$(a + ib)(u + iv) = (au - bv) + i(av + bu),$$

$u + iv \in V + iV$. So this is similar to how we get new elements when we extend from $\mathbb{R}$ to $\mathbb{C}$. If V is n-dimensional, with basis $\{ e_1, ..., e_n \}$, then $\mathbb{C} \otimes V$ is n-dimensional $\mathbb{C}$-vector space with basis $\{ e_1, ..., e_n \}$ and $2n$-dimensional $\mathbb{R}$-vector space with basis $\{ e_1, ..., e_n, ie_1, ..., ie_n \}$. Now let T be a linear transformation of V. Then V is an $\mathbb{R}[x]$-module by $xu = Tu$. We have:

$$\left(\sum_{k=0}^{n} a_k x^k \right) u = \sum_{k=0}^{n} a_k T^k u.$$

So $\mathbb{C}[x] \otimes_{\mathbb{R}[x]} V$ is a $\mathbb{C}[x]$-module, that is, we have a $\mathbb{C}$-vector space $\mathbb{C} \otimes_{\mathbb{R}} V$ on which T acts as a linear transformation.

(3) Let A_1, A_2 be R-algebras. Then $A_1 \otimes_R A_2$ has a structure of an R-algebra by

$$\alpha_1 \otimes \beta_1) \cdot (\alpha_2 \otimes \beta_2) = (\alpha_1 \alpha_2) \otimes (\beta_1 \otimes \beta_2).$$

Shit should be checked, but it works. The **subscript below the tensor product symbol** represents where the scalars are from.

(4) *This is a problem from the book. If S is an R-algebra, prove that $S \otimes_R R[x] \cong S[x]$.*

PROOF. You need to check something like this:

$$(\alpha_1 \otimes (a_1 x^n + \cdots + a_1 x + a_0)) \cdot (\alpha_2 \otimes (...)).$$

The map would be given by:

$$\alpha_1 \otimes (a_1 x^n + \cdots + a_1 x + a_0) \mapsto a_n \alpha x^n + \cdots a_1 \alpha x + a_0 \alpha.$$

Here it is just defined for simple tensors. So any polynomial of S is the image of some tensor, since we have:

$$\alpha_n \otimes x^n + \cdots + \alpha_1 \otimes x + \alpha_0 \otimes 1 \mapsto \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0.$$

□

(5) Prove $R[x] \otimes_R R[y] \cong R[x, y]$.

PROOF.

$$(a_n x^n + \cdots a_1 x + a_0) \otimes (b_m y^m + \cdots + b_1 y + b_0) \mapsto a_n b_m x^n y^n + \cdots + a_0 b_0 = p(x) q(x).$$

We map $x^n \otimes y^m \mapsto x^n y^m$. Again this is an exercise from the book. □

DEFINITION 1.109. Let $\varphi_1 \in Hom(M_1, N_1)$ and $\varphi_2 \in Hom(M_2, N_2)$. Then $\varphi_1 \otimes \varphi_2 : M_1 \otimes M_2 \to N_1 \otimes N_2$. is defined by $\varphi_1 \otimes \varphi_2(u_1 \otimes u_2) = \varphi_1(u_1) \otimes \varphi_i(u_2)$. This is the **tensor product of two homomorphisms.**

We prove it is a homomorphism.

PROOF. It is well defined since the mapping $(u_1, u_2) \mapsto \varphi_1(u_1) \otimes \varphi_2(u_2)$ is bilinear. So we get a mapping $Hom(M_1, N_1) \times Hom(M_2, N_2) \to Hom(M_1 \otimes M_2, N_1 \otimes N_2)$. This mapping is also bilinear. We have to check four identities. So it defines a homomorphism:

$$Hom(M_1, N_1) \otimes Hom(M_2, N_2) \to Hom(M_1 \otimes M_2, N_1 \otimes N_2),$$

as we have seen from the definition/construction of a tensor product. □

DEFINITION 1.110. Assume that M is an R-module. We want to convert it to an algebra. If we take $M \otimes M$, then we multiply two vectors, but we cannot multiply these tensors. To have an algebra you must be able to multiply any elements. So if we want an algebra, we take $R \oplus M \oplus (M \otimes M) \oplus (M \otimes M \otimes M) \oplus (...) \oplus \cdots$. This is called the **tensor algebra of M.**

DEFINITION 1.111. An **graded algebra**:

$$A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots,$$

such that $\forall i, j,\ A_i \cdot A_j \subseteq A_{i+j}$.

EXAMPLE 1.112. We give a neat example that demonstrates why the location of the scalars is important:

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}^4,$$

$$\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C} \cong \mathbb{R}^2.$$

REMARK 1.113. In the case $M = M_1 \oplus M_2$, where M_1 is free, M_2 is torsion. Not always the case, but it is in PID, or in finitely generated abelian groups. So $F \otimes M = F \otimes M \oplus 0$. It has the same rank as M_1. If $M_1 = R^n$, then $F \otimes M_1 \cong F^n$, and it is a vector space. So this operation **kills all torsion.**

REMARK 1.114. Recall that an **R-algebra** is basically an R-module which is also a ring. So it is an R-module with multiplication.

Friday, January 26th
We do some exercises from the book starting with 10.4.8.
Monday, January 29th
We go to Section 10.5.

10.4 Exercises

8. *Let R be an integral domain, Q-field of quotients, N an R-module, and $U = R^* = R - \{ 0 \}$. We define: $U^{-1}N = U \times N/\sim$. Where:*

$$(u, n) \sim (u', n') \text{ if } v(u'n - un') = 0,$$

for some v. Denote $(u, n) = \frac{n}{u}$. We define addition:

$$\frac{n}{u} + \frac{m}{v} = \frac{vn + um}{uv}.$$

And we define multiplication by scalars:

$$r\frac{n}{u} = \frac{rn}{u}.$$

And we claim that $U^{-1}N$ becomes an R-module.

(a) PROOF. We have:

$$\begin{gathered}(u, n) \sim (u', n') \sim (u'', n'') \Rightarrow^{?} (u, n) \sim (u'', n''), \\ u'n = un', u''n' = u'n'' \Rightarrow^{?} un'' = u''n.\end{gathered} \tag{1.25}$$

But we have $u''u'n = u''un' = uu'n''$, so $u'(u''n - un'') = 0$. So the relation given by the book, $u'n - un'$ must be the wrong one, so we now switch to using the relation stated above. So we have:

$$\begin{aligned} &(u,n) \sim (u',n') \sim (u'',n'') \Rightarrow^{?} (u,n) \sim (u'',n''), \\ &nu'n = nun', n'u''n' = v'u'n'' \Rightarrow^{?} . \end{aligned} \tag{1.26}$$

So we have $vv'u''u'n = vv'u''un' = vv'uu'n''$, so $vv'u'(u''n - un'') = 0$. So $(u,n) \sim (u'',n'')$. If $(n,u) \sim (n',u'), (m,v) \sim (m',v')$ is $(uv, vn + um) \sim (u'v', v'n' + u'm')$. Is this true? Leibman thinks so. Let's believe that this is true. Or not. Let's check. So we have $w(mv' - m'v) = 0$ for some $w \neq 0$. And $w'(nu' - n'u) = 0$ for some $w' \neq 0$. Now we take

$$ww'(uv(v'n' + u'm') - u'v'(un + um)) = ww'[vv'(un' - u'n) + uu'(vm' - v'm)] = 0. \tag{1.27}$$

And then we have to check something else, which we will skip. So $U^{-1}N$ is an R-module, $U^{-1}N = \left\{ \frac{n}{u}, n \in N, u \in R - \{ 0 \} \right\}$. Up until this point, we only needed that R is commutative, and that U is multiplicatively closed, we did not need that R was integral domain yet.

□

(b) *Prove that $U'N \cong Q \otimes_R N$.*

Proof. Define $\varphi : Q \otimes_R N \to U^{-1}N$ by $\frac{a}{b} \otimes n \mapsto \frac{an}{b}$. Of course it is a well-defined homomorphism, it can be easily checked. Can we construct an inverse? Define $\psi : U^{-1}N \to Q \otimes_R N$ by $\frac{n}{u} \mapsto \frac{1}{u} \otimes n$. And check that $\psi = \varphi^{-1}$. Well, is it well-defined? We don't have to check that it is a homomorphism, since if it is the inverse of one, then it is one itself. If $(n',u') \sim (n,u)$, is $\frac{1}{u} \otimes n' = \frac{1}{u} \otimes n$? Let $v(un' - u'n) = 0$. Then:

$$\begin{aligned} \frac{1}{u'} \otimes n' &= uv \cdot \left(\frac{1}{uvu'} \otimes n' \right) \\ &= \frac{1}{uvu'} \otimes uvn' \\ &= \frac{1}{uvu'} \otimes u'vn \\ &= \frac{1}{u} \otimes n. \end{aligned} \tag{1.28}$$

So it's well defined. Now why is it the inverse of φ. Observe:

$$\begin{aligned} &\frac{n}{u} \overset{\psi}{\mapsto} \frac{1}{u} \otimes n \overset{\varphi}{\mapsto} \frac{n}{u}, \\ &\frac{v}{u} \otimes n = v(\frac{1}{u} \otimes n) \overset{\varphi}{\mapsto} v \cdot \frac{n}{u} \overset{\psi}{\mapsto} \frac{1}{u} \otimes vn = \frac{v}{u} \otimes n. \end{aligned} \tag{1.29}$$

□

(c) *Prove that $\frac{1}{d} \otimes n = 0$ if and only if $rn = 0$ for some $r \in R^*$.*

Proof. Under the isomorphism from part (b) we have:

$$\frac{1}{d} \otimes n \overset{\varphi}{\mapsto} \frac{n}{d} \in U^{-1}N.$$

And $\frac{n}{d} = 0 = \frac{0}{1}$ if and only if $r(n - 0) = 0$ for some $r \neq 0$. And we make use of this result in Exercise 10.4.9. □

(d) *Let A be an abelian group. Then prove $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$ if and only if A is a torsion group, $|a| < \infty \ \forall a \in A$.*

PROOF. We claim that $\mathbb{Q} \otimes N = 0$ if and only if $N = Tor(N)$. If $N = Tor(N)$, then $Q \otimes N = 0$. Recall that A being abelian is equivalent to saying it is a $\mathbb{Z}$-module. So $R = \mathbb{Z}$ in this case, so $\mathbb{Q} = Q$, the field of fractions of the ring. If $N = Tor(N)$, then $Q \otimes N = 0$. If $Q \otimes N = 0$, then $\forall n \in N$, $1 \otimes n = 0 <$ so $\exists r \neq 0$, s.t. $rn = 0$ by part (c). So $n \in Tor(N)$ for all n. □

9. *Suppose R is an integral domain with quotient field Q and let N be any R-module. Let $Q \otimes_R N$ be the module obtained from N by extension of scalars from R to Q. Prove that the kernel of the R-module homomorphism $\iota : N \to Q \otimes_R N$ is the torsion submodule of N. [Exercise 10.1.8.,Exercise 10.4.8]*

PROOF. Recall that the torsion submodule is defined as:

$$Tor(N) = \{n \in N : rn = 0 \text{ for some nonzero } r \in R\}.$$

And recall that $\iota(n) = 1 \otimes n$. Let $n \in Tor(N)$. Then $\iota(n) = 1 \otimes n$. Since $n \in Tor(N)$, there exists $r \neq 0$ such that $rn = 0$, and we also have $1/r \in Q$. So we have:

$$1 \otimes n = 1(1 \otimes n) = \frac{1}{r} r(1 \otimes n) = \frac{1}{r}(1 \otimes rn) = \frac{1}{r}(1 \otimes 0) = 0.$$

Thus $n \in ker\iota$, and $Tor(N) \subseteq ker\iota$. Now let $n \in ker\iota$. Then

$$\iota(n) = 1 \otimes n = 0 = 1 \otimes 0.$$

So we must have that there exists $r \neq 0$ s.t. $rn = 0$. And by the result of Exercise 10.4.8(c), we know that $(1/d) \otimes n = 0$ if and only if there exists $r \in R$ s.t. $rn = 0$. Hence we know $n \in Tor(N)$. □

10. *Suppose R is commutative and $N \cong R^n$ is a free R-module of rank n with R-module basis $e_1, ..., e_n$.*

Recall the definition of a free module of rank n:

DEFINITION 1.115. A **free module** is a direct sum of finitely or infinitely many copies of R,

$$F_\Lambda = \bigoplus_{\alpha \in \Lambda} R = \{a_{\alpha_1} + \cdots + a_{\alpha_k} : k \in \mathbb{N}, \alpha_i \in \Lambda, a_{\alpha_i} \in R\},$$

where the sum of u's above is a formal sum. We can also define it as:

$$F_\Lambda = \{(a_\alpha)_{\alpha \in \Lambda} : a_\alpha \in R, \forall \alpha, a_\alpha = 0 \text{ for all but finitely many } \alpha\}.$$

Note R is unital here.

(a) *For any nonzero R-module M show that every element of $M \otimes N$ can be written uniquely in the form $\sum_{i=1}^n m_i \otimes e_i$ where $m_i \in M$. Deduce that if $\sum_{i=1}^n m_i \otimes e_i = 0$ in $M \otimes N$, then $m_i = 0$ for $i = 1, ..., n$.*

PROOF. Let $t = a_1(u_1 \otimes v_1) + \cdots + a_l(u_l \otimes v_l) \in M \otimes N$. And for each $v_i \in N$ we have:

$$v_i = r_1 e_1 + \cdots + r_n e_n,$$

with $r_j \in R$ uniquely by the definition of our standard basis. Then we may write:

(1.30)
$$\begin{aligned} t &= a_1(u_1 \otimes (r_{1,1}e_1 + \cdots + r_{1,n}e_n)) + \cdots + a_l(u_l \otimes (r_{l,1}e_1 + \cdots + r_{l,n}e_n)) \\ &= (a_1u_1 \otimes (r_{1,1}e_1 + \cdots + r_{1,n}e_n)) + \cdots + (a_lu_l \otimes (r_{l,1}e_1 + \cdots + r_{l,n}e_n)) \\ &= ((a_1u_1 \otimes r_{1,1}e_1) + \cdots + (a_1u_1 \otimes r_{1,n}e_n)) + \cdots + ((a_lu_l \otimes r_{l,1}e_1) + \cdots + (a_lu_l \otimes r_{l,n}e_n)) \\ &= ((a_1r_{1,1}u_1 \otimes e_1) + \cdots + (a_1r_{1,n}u_1 \otimes e_n)) + \cdots + ((a_lr_{l,1}u_l \otimes e_1) + \cdots + (a_lr_{l,n}u_l \otimes e_n)) \\ &= ((a_1r_{1,1}u_1 \otimes e_1) + \cdots + (a_lr_{l,1}u_l \otimes e_1)) + \cdots + ((a_1r_{1,n}u_1 \otimes e_n) + \cdots + (a_lr_{l,n}u_l \otimes e_n)) \\ &= ((a_1r_{1,1}u_1 \cdots + a_lr_{l,1}u_l) \otimes e_1) + \cdots + ((a_1r_{1,n}u_1 + \cdots + a_lr_{l,n}u_l) \otimes e_n). \end{aligned}$$

So letting $m_i = (a_1r_{1,i}u_1 \cdots + a_lr_{l,i}u_l)$, we have:

$$t = \sum_{i=1}^{n} m_i \otimes e_i,$$

where $m_i \in M$. Assume that $\sum_{i=1}^{n} m_i \otimes e_i = 0$. If each term in the sum is identically zero, then the result is proved, all $m_i = 0$. So without loss of generality, assume $m_1, ..., m_k \neq 0$ for some $k \leqslant n$. If the m_i's are linearly independent, then since the e_i's are also linearly independent:

$$\sum_{i=1}^{n} m_i \otimes e_i = 0 \Rightarrow m_i = 0, \forall i,$$

which is a contradiction. So then we must have that the m_i's are linearly dependent. So we can write:

$$\sum_{i=1}^{k} m_i \otimes e_i = \sum_{i=1}^{k} r_i m \otimes e_i = \sum_{i=1}^{k} m \otimes r_i e_i = 0.$$

If $m = 0$ we are done, contradiction, since then $m_i = 0$ for all i. If $\sum r_i e_i = 0$ we have a contradiction, since then the basis wouldn't be linearly independent. So we must have that all $m_i = 0$. □

(b) *Show that if $\sum m_i \otimes n_i = 0$ in $M \otimes N$ where the n_i are merely assumed to be R-linearly independent, then it is not necessarily true that all the m_i are 0. [Consider $R = \mathbb{Z}, n = 1, M = \mathbb{Z}/2\mathbb{Z}$, and the element $1 \otimes 2$.]*

Proof. Note that now we relax the assumption that our elements from R^n generate R^n. So now they are only linearly independent. We have:

$$1 \otimes 2 = 2 \otimes 1 = 0 \otimes 1 = 0,$$

but $1 \neq 0 \in \mathbb{Z}/2\mathbb{Z}$, and 2 is just a single element of some R module over R, so it is linearly independent. So we have found a counterexample. □

15. *Prove that $M \otimes (N \oplus K) \cong (M \otimes N) \oplus (M \otimes K)$. The same is true for:*

$$M \otimes \left(\bigoplus_{\alpha \in \Lambda} N_\alpha \right) \cong \bigoplus_{\alpha \in \Lambda} (M \otimes N_\alpha),$$

which uses the same proof. But:

$$M \otimes \left(\prod_{\alpha \in \Lambda} N_\alpha \right) \ncong \prod_{\alpha \in \Lambda} (M \otimes N_\alpha).$$

Example: $R = \mathbb{Z}, M = \mathbb{Q}, N_i = \mathbb{Z}_{2^i}, i = 1, 2, ...$ Consider:

$$\mathbb{Q} \otimes \left(\prod_{i=1}^{\infty} \mathbb{Z}_{2^i} \right) \neq 0,$$

by 8. But note:

$$\prod_{i=1}^{\infty} (\mathbb{Q} \otimes \mathbb{Z}_{2^i}) = 0.$$

16. *Suppose R is commutative and let I and J be ideals of R, so $R/I, R/J$ are naturally R-modules .*

(a) *Prove that every element of $R/I \otimes_R R/J$ can be written as a simple tensor of the form $(1 \mod I) \otimes (r \mod J)$.*

PROOF. Let:

$$t = a_1(b_1 \mod I \otimes c_1 \mod J) + \cdots + a_l(b_l \mod I \otimes c_l \mod J) \in R/I \otimes_R R/J,$$

with $a_i, b_i, c_i \in R$. Then we have:

$$\begin{aligned} t &= a_1 b_1 (1 \mod I \otimes c_1 \mod J) + \cdots + a_l b_l (1 \mod I \otimes c_l \mod J) \\ &= (1 \mod I \otimes a_1 b_1 c_1 \mod J) + \cdots + (1 \mod I \otimes a_l b_l c_l \mod J) \\ &= 1 \mod I \otimes (a_1 b_1 c_1 + \cdots + a_l b_l c_l) \mod J, \end{aligned} \tag{1.31}$$

so since $(a_1 b_1 c_1 + \cdots + a_l b_l c_l) \in R$, we have written t as a simple tensor. □

(b) *Prove that there is an R module isomorphism $R/I \otimes_R R/J \cong R/(I+J)$ mapping $(r \mod I) \otimes (r' \mod J)$ to $rr' \mod (I+J)$.*

PROOF. Let $\varphi : R/I \otimes_R R/J \to R/(I+J)$ be given by $\varphi((r \mod I) \otimes (r' \mod J)) = rr' \mod (I+J)$. We prove this is an isomorphism. Since we proved that every element of $R/I \otimes_R R/J$ can be written as a simple tensor of the form $(1 \mod I) \otimes (r \mod J)$, we need only to check elements of this form.

Homomorphism: We have:

$$\begin{aligned} &\varphi((1 \mod I) \otimes (r \mod J) + (1 \mod I) \otimes (s \mod J)) \\ =&\varphi((1 \mod I) \otimes (r+s \mod J)) \\ =&r+s \mod (I+J) \\ =&r \mod (I+J) + s \mod (I+J) \\ =&\varphi((1 \mod I) \otimes (r \mod J)) + \varphi((1 \mod I) \otimes (s \mod J)). \end{aligned} \tag{1.32}$$

So addition is preserved, and for $a \in R$, we also have:

$$\begin{aligned} \varphi(a((1 \mod I) \otimes (r \mod J))) &= \varphi(((a \mod I) \otimes (r \mod J))) \\ &= ar \mod (I+J) \\ &= a(r \mod (I+J)) \\ &= a\varphi((1 \mod I) \otimes (r \mod J)). \end{aligned} \tag{1.33}$$

So φ is an R-module homomorphism.

Injectivity: Observe:

$$\varphi((1 \mod I) \otimes (r \mod J)) = \varphi((1 \mod I) \otimes (s \mod J)), \tag{1.34}$$

which gives us:

$$r \mod (I+J) = s \mod (I+J), \tag{1.35}$$

thus we know $r - s \in (I + J)$. So $r - s = j \mod I$ for some $j \in J$. So we have:

$$\begin{aligned}
&(1 \mod I) \otimes (r \mod J) - (1 \mod I) \otimes (s \mod J) \\
=&(1 \mod I) \otimes (r - s \mod J) \\
=&(r - s \mod I) \otimes (1 \mod J) \\
=&(j \mod I) \otimes (1 \mod J) \\
=&(1 \mod I) \otimes (j \mod J) \\
=&0.
\end{aligned} \tag{1.36}$$

So φ must be injective.

Surjectivity: Let $r \mod (I + J) \in R/(I + J)$. Then $\varphi((1 \mod I) \otimes (r \mod J)) = r \mod (I + J)$, so φ is surjective. Hence φ is an isomorphism. □

20. *Let $I = (2, x)$ be the ideal generated by 2 and x in the ring $R = \mathbb{Z}[x]$. Show that the element $2 \otimes 2 + x \otimes x$ in $I \otimes_R I$ is not a simple tensor, i.e., cannot be written as $a \otimes b$ for some $a, b \in I$.*

Proof. Define $t = 2 \otimes 2 + x \otimes x$. We first express t as a simple tensor in R. We define $\beta : \mathbb{Z}[x] \times \mathbb{Z}[x] \to \mathbb{Z}[x] \otimes \mathbb{Z}[x]$ given by $\beta((p(x), q(x)) = p(x) \otimes q(x)$. We also define $\gamma : \mathbb{Z}[x] \times \mathbb{Z}[x] \to \mathbb{Z}[x]$ given by $\gamma((p(x), q(x)) = p(x)q(x)$. This map is bilinear, so we have an induced homomorphism $\varphi : \mathbb{Z}[x] \otimes \mathbb{Z}[x] \to \mathbb{Z}[x]$, so altogether, we have:

$$\begin{array}{ccc}
 & \mathbb{Z}[x] \times \mathbb{Z}[x] & \\
{\scriptstyle\beta}\swarrow & & \searrow{\scriptstyle\gamma} \\
\mathbb{Z}[x] \otimes \mathbb{Z}[x] & \xrightarrow{\quad\varphi\quad} & \mathbb{Z}[x]
\end{array}.$$

Then we would have:

$$p \otimes q = 2 \otimes 2 + x \otimes x,$$

for some $p, q \in \mathbb{Z}[x]$. But we also know:

$$2 \otimes 2 + x \otimes x = 4(1 \otimes 1) + x \otimes x = 4(1 \otimes 1) + x^2(1 \otimes 1) = (4 + x^2)(1 \otimes 1) \in \mathbb{Z}[x]$$

But $(4 + x^2)$ is a prime in $\mathbb{Z}[x]$. To write t as a simple tensor in $\mathbb{Z}[x]$, we must have $4 + x^2 = ab$ for some $a, b \in \mathbb{Z}[x]$, so that we may write:

$$ab(1 \otimes 1) = a \otimes b \in \mathbb{Z}[x].$$

So let $4 + x^2 = ab$, and since it is a prime and we are in $\mathbb{Z}[x]$, without loss of generality, we must have $b = 1$, but note that $1 \notin I$, so it is impossible to write t as a simple tensor in $I \otimes_R I$, since under the same bilinear map γ, we have:

$$\begin{array}{ccc}
 & I \times I & \\
{\scriptstyle\beta}\swarrow & & \searrow{\scriptstyle\gamma} \\
I \otimes I & \xrightarrow{\quad\varphi\quad} & I^2
\end{array},$$

from which we see that the image $u \otimes v \mapsto uv$ of any simple tensor is reducible. □

21. *Suppose R is commutative, and let I and J be ideals of R.*

(a) *Show that there is a surjective R-module homomorphism from $I \otimes_R J$ to the product ideal IJ mapping $i \otimes j$ to the element ij.*

PROOF. Let $\varphi : I \otimes_R J \to IJ$ be given by:

$$\varphi(r_1(i_1 \otimes j_1) + \cdots + r_n(i_n \otimes j_n)) = r_1 i_1 j_1 + \cdots + r_n i_n j_n.$$

We show that φ is a surjective homomorphism of R-modules. Observe:

$$\begin{aligned}
&\varphi((r_1(i_1 \otimes j_1) + \cdots r_n(i_n \otimes j_n)) + (s_1(i'_1 \otimes j'_1) + \cdots s_m(i'_m \otimes j'_m))) \\
=&\varphi(r_1(i_1 \otimes j_1) + \cdots r_n(i_n \otimes j_n) + s_1(i'_1 \otimes j'_1) + \cdots s_m(i'_m \otimes j'_m)) \\
=&r_1 i_1 j_1 + \cdots + r_n i_n j_n + s_1 i'_1 j'_1 + \cdots + s_m i'_m j'_m \\
=&\varphi((r_1(i_1 \otimes j_1) + \cdots r_n(i_n \otimes j_n)) + \varphi((s_1(i'_1 \otimes j'_1) + \cdots s_m(i'_m \otimes j'_m))).
\end{aligned} \tag{1.37}$$

So φ preserves addition. Additionally:

$$\begin{aligned}
\varphi(r(i \otimes j)) &= \varphi((ri \otimes j)) \\
&= rij \\
&= r\varphi((i \otimes j)).
\end{aligned} \tag{1.38}$$

So φ also preserves scalar multiplication for simple tensors and thus for general tensors as well. Now we show that φ is surjective. Let $r \in IJ$. Then

$$r = \sum_{k=1}^{n} i_k j_k,$$

for $i_k \in I, j_k \in J$. Then $\varphi(i_1 \otimes j_1 + \cdots + i_n \otimes j_n) = r$, because we already proved φ is a homomorphism and hence preserves addition, so φ is surjective. □

(b) *Give an example to show that the map in (a) need not be injective [Exercise 10.4.17].*

Consider $I = (2, x)$ and $R = \mathbb{Z}[x]$. We define a map: $\varphi : I \otimes_R I \to II = I$ given by $\varphi(i \otimes j) = ij$. By part (a), we know it is a surjective homomorphism. Note:

$$\varphi(2 \otimes x) = \varphi(x \otimes 2) = 2x.$$

But from Exercise 10.4.17(c), we know that $2 \otimes x \neq x \otimes 2$ in $I \otimes_R I$.

1.5. Exact Sequences and Tensor Algebras

Monday, January 29th

DEFINITION 1.116. Let M be an R-module. $\forall k \in \mathbb{N}$ let $\tau_k(M) = M \otimes \cdots \otimes M$ (k-times). These are called the set of k-tensors. Note that $\tau_0(M) = R$ and $\tau_1(M) = M$. We have:

$$\tau(M) = \bigoplus_{K=0}^{\infty} \tau_k(M),$$

called the **tensor algebra of** M.

Elements look like sums:

$$a + u_1 + b_2(u_2 \otimes u_3) + b_3(u_5 \otimes u_6 \otimes u_7) + \cdots + d_8(u_9 \otimes u_{10}).$$

DEFINITION 1.117. **Universal Property:** if A is an R=algebra and $\varphi : M \to A$ is a hom-sm of R-modules, then $\exists$ a unique hom-sm $\Phi : \tau(M) \to A$ of R-algebras such that:

$$\Phi|_{M=\tau_1(M)} = \varphi, \Phi(u_1 \otimes \cdots \otimes u_k) \quad = \varphi(u_1) \cdots \varphi(u_k) \in A. \tag{1.39}$$

EXAMPLE 1.118. (1) Let $M = R$. Then we have $\tau(R) = R \oplus R \oplus R \cdots$. The elements are finite multiplications. Let's artificially introduce basis vector. Let $M = Rx$, $(x = 1)$. Where x is the basis vector. Then

$$\begin{aligned} \tau_1(R) &= Rx, \\ \tau_2(R) &= R \otimes R = R(x \otimes x), \\ \tau_3(R) &= R(x \otimes x \otimes x), \\ \tau(R) &= R \oplus R \otimes R \oplus R \otimes R \otimes R \oplus \cdots \cong R[x]. \end{aligned} \tag{1.40}$$

(2) $M = R^2 = R\{ x, y \}$. Then:

$$\tau(R) \cong \{ \text{ polynomials in non-commutative variables x and y. } \} = RG,$$

since $x \otimes y \neq y \otimes x$. where G is the free semigroup generated by x, y:

$$G = \left\{ 1, x, y, x^2, xy, yx, y^2, xyx, ... \right\}.$$

DEFINITION 1.119. **Symmetric algebra of** M. Let $\mathcal{C}(M)$ be the ideal in $\tau(M)$ generated by $u \otimes v - v \; tensu, u, v \in M$. The algebra $\mathcal{S}(M) = \tau(M)/\mathcal{C}(M)$ is called the **symmetric algebra of** M**.**

So in the above definition, we just declare that $x \otimes y = y \otimes x$, and you can switch them along any chain of tensor products:

$$u_1 \otimes u_2 \otimes u_3 \otimes u_4 = u_4 \otimes u_2 \otimes u_3 \otimes u_1 \in \mathcal{S}(M).$$

The ability to do it on more than two tensors follows from the structure of transpositions in symmetric groups. What even is a higher degree tensor? We prove something:

PROOF. $\forall k$ S_k acts of $\tau_k(M)$ by $\sigma(u_1 \otimes \cdots u_k) = u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(k)}$. The action of any transposition is trivial module $\mathcal{C}(M)$ or something like that. □

DEFINITION 1.120. **Universal Property:** If A is a commutative R-algebra, and $\varphi : M \to A$ is a hom-sm of R-modules, then there is a unique hom-sm $\Phi : \mathcal{S}(M) \to A$ such that $\Phi|_M = \varphi$. Also $\mathcal{S}(M)$ is still a **graded algebra** (Definition 1.4):

$$\mathcal{S}(M) = R \oplus \mathcal{S}_1(M) \oplus \mathcal{S}_2(M) \oplus \cdots$$

where the second term is $\cong M$. Why is it unique? Because we have no choice as to send $\Phi(u_1 \otimes \cdots u_k) = \varphi(u_1) \cdots \varphi(u_k)$.

EXAMPLE 1.121. Take M to be the free module generated by two elements $M = R\{ x, y \}$. And then $\mathcal{S}(M) \cong R[x, y]$ (now we have commutativity!).

DEFINITION 1.122. **Exterior Algebra:** let $A(M)$ be the ideal in $\tau(M)$ generated by tensors $u \otimes u$, $u \in M$. The algebra:

$$\Lambda(M) = \tau(M)/A(M),$$

is called the exterior algebra of M.

In $\Lambda(M)$, instead of $\otimes$, we write "$\wedge$" - wedge. So we have:

$$\Lambda(M) = \{\, a + u_1 + u_2 \wedge u_3 + u_4 \wedge u_5 \wedge u_6 + \cdots () \,\}.$$

In $\Lambda(M)$, $u \wedge u = 0$ for all u, and:

$$u \wedge v = -v \wedge u.$$

Proof.

$$(u+v) \wedge (u+v) = u \wedge u + u \wedge v + v \wedge u + v \wedge v.$$

□

$\int f dx \neq \int f(\varphi(t))dt$. But we do have:

$$\int f dx = \int f(\varphi(t))\varphi'(t)dt.$$

$f dx$ is called the **differential form**. And we have $\int f(x,y)dx \wedge dy$, where $f(x,y)dx \wedge dy$ is called a differential form of second order. Recall:

$$\int f(x,y)dx \wedge dy = \int f(x(u,v), y(u,v)) \cdot |J| du \wedge dv.$$

Where $|J|$ is the Jacobian of $(u,v) \mapsto (x,y)$ as vertical vectors.

Bonus Problem: If $x = au + bv$ and $y = cu + dv$ prove that $x \wedge y = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} u \wedge v$.

Now what the hell is going on when our ring is **noncommutative**. Let M, N be a left R-module. Can you have:

$$(au) \otimes v = u \otimes av?$$

But then we have the following:

$$(abu) \otimes v = (bu) \otimes (av) = u \otimes (bav) = (bau) \otimes v.$$

So we have some weird new hidden relations. So now:

$$ab(u \otimes v) = ba(u \otimes v),$$

R acts on $M \otimes N$ as a commutative ring.

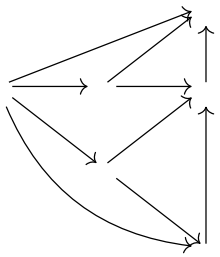
Remark 1.123. If M is a right R-module and N is a left R-module, product $M \otimes_R N$ where:

$$(ua) \otimes v = u \otimes (av),$$

and this will be okay, no problem like this. But you cannot take scalars out. So it is not equal to $a(u \otimes v)$. It is an abelian group only, not an R-module. Mappings with this property are called **balanced maps** since they are missing one of the four bilinearity properties.

Tuesday, January 30th

Definition 1.124. A diagram of sets and mappings is a **commutative diagram** if for all paths with common starting and ending points, the composition of mappings along these paths is the the same.



DEFINITION 1.125. A sequence $A_{i-1} \to^{\varphi_{i-1}} A_i \to^{\varphi_i} A_{i+1} \to^{\varphi_{i+1}} A_{i+2} \to$ of hom-sms of groups, rings, or modules is **exact** if $\forall i\ Image(\varphi_i) = ker(\varphi_{i+1})$.

REMARK 1.126. $0 \to A \to_\varphi B$ is exact if and only if φ is injective. $(ker(\varphi) = Image(0))$

REMARK 1.127. $B \to_\psi C \to 0$ is exact if and only if φ is surjective. $(\psi(B) = ker(C \to 0) = C)$

REMARK 1.128. The sequence $0 \to A \to_\varphi B \to_\psi C \to 0$ is exact (a **short exact sequence**) if and only if φ is injective (monomorphism),ψ is surjective (epimorphism), and $\varphi(A) = ker(\psi)$. So we have $C \cong B/\varphi(A)$, $\varphi(A) \cong A$.

For groups: $1 \to A \to B \to C \to 1$, $C \cong B/A$.

DEFINITION 1.129. The short exact sequence **splits** if there exists a hom-sm $\sigma : C \to B$ called a **section**, such that $\psi \circ \sigma = Id_C$. So we have:

$$0 \longrightarrow A \xrightarrow[\varphi]{} B \underset{\psi}{\overset{\sigma}{\rightleftarrows}} C \longrightarrow 0$$

In this case, then $B \cong A \oplus C$,

$$B = \varphi(A) \oplus \sigma(C),$$

with an internal direct product.

PROOF. $\forall b \in B$:

$$\begin{aligned} \psi(b - \sigma(\psi(b))) &= \psi(b) - \psi \circ \sigma(\psi(b)) \\ &= \psi(b) - \psi(b) = 0. \end{aligned} \tag{1.41}$$

So $b - \sigma(\psi(b)) \in \varphi(A)$, so $b = \sigma(c) + \varphi(a)$ for $c = \psi(b)$ and some $a \in A$. If $\varphi(a) = \sigma(c)$, then:

$$0 = \psi(\varphi(a)) = \psi(\sigma(c)) = c,$$

so $\sigma(c) = 0$, and $\varphi(a) = 0$, so $\sigma(C) \cap \varphi(A) = 0$. □

DEFINITION 1.130. A homomorphism of two short exact sequences is a commutative diagram of the sort:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array},$$

with exact rows.

LEMMA 1.131 (**SHORT FIVE LEMMA**). *Let:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\varphi'} & B' & \xrightarrow{\psi'} & C' & \longrightarrow & 0 \end{array},$$

be a homomorphism of short exact sequences.

(a) If α and γ are surjective, then β is surjective.
(b) If α and γ are injective, then β is injective.
(c) If α and γ are isomorphisms, then β is an isomorphism.

PROOF. **(b)** We make use of the diagram! Let α,γ be injective. Let $b \in B$, and assume that $\beta(b) = 0$. Consider:

$$\gamma(\psi(b)) = \psi'(\beta(b)) = \psi'(0) = 0. \tag{1.42}$$

But γ is injective, so $\psi(b) = 0$. But the first row is exact, so $b = \varphi(a)$ for some $a \in A$. Then:

$$\varphi'(\alpha(a)) = \beta(\varphi(a)) = \beta(b) = 0, \tag{1.43}$$

But φ', α are injective, so $a = 0$, so $b = \alpha(a) = 0$. □

PROOF. **(a)** Let α, γ be surjective. Let $b' \in B'$ (we need tos how that $b' = \beta(b)$ for some $b \in B$). So take $\psi'(b')$ but then since this is in C' and γ is surjective, so there exists $c \in C$ such that $\gamma(c) = \psi'(b')$. Next, ψ is surjective, so we have $\hat{b} \in B$ such that $\psi(\hat{b}) = c$. So we have:

$$\gamma(c) = \gamma(\psi(\hat{b})) = \psi'(b').$$

Consider:

$$\psi'(b' - \beta(\hat{b})) = \psi'(b') - \psi'(\beta(\hat{b})) = \gamma(c) - \gamma(\psi(\hat{b})) = 0.$$

The second row is exact, so $\exists a' \in A'$ such that:

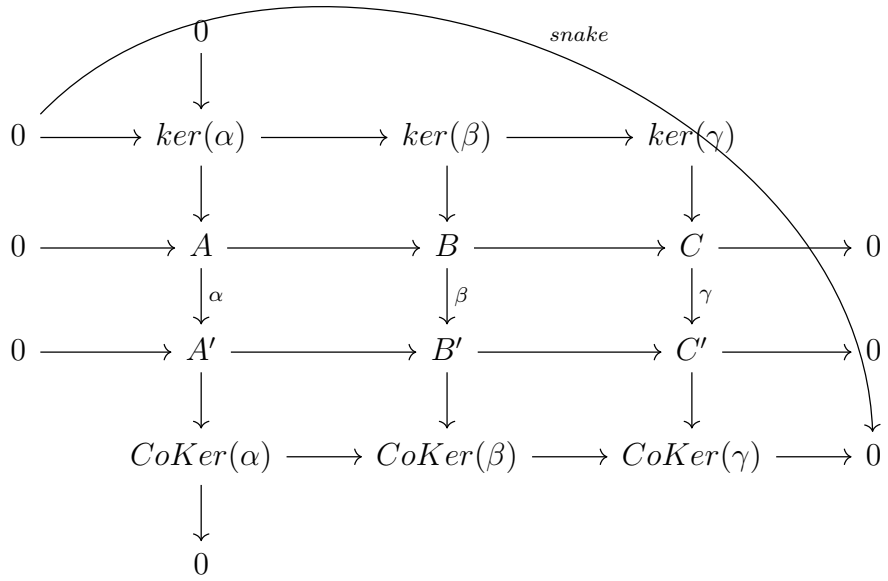
$$\varphi'(a') = b' - \beta(\hat{b}),$$

α is surjective, so $\exists a \in A$ such that $a' = \alpha(a)$. **If a row is exact, this means the image of first map is the kernel of the second map.** Take $b = \hat{b} + \varphi(a)$. Then:

$$\beta(b) = \beta(\hat{b}) + \beta(\varphi(a)) = \beta(\hat{b}) + \varphi'(\alpha(a)) = \beta(\hat{b}) + b' - \beta(\hat{b}) = b'. \tag{1.44}$$

Part (c) is a corollary of the others. □

LEMMA 1.132 (**SNAKE LEMMA**). *$CoKer(\alpha) = A'/\alpha(A)$. We have a commutative diagram with exact rows and columns:*



Then there exists a homomorphism $\delta : ker\gamma \to ker\alpha$ such that the snake is exact.

Wednesday, January 31st

REMARK 1.133. Let M be an R-module. Let A be a submodule of module B. Then it may be that $A \otimes M$ is not a submodule of $B \otimes M$!

Consider:

$$0 \longrightarrow A \xrightarrow{\varphi} B$$

which is exact! Then we have:

$$0 \longrightarrow A \otimes M \xrightarrow{\varphi \otimes Id_M} B \otimes M \ ,$$

which may not be exact.

EXAMPLE 1.134. In $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$ we have:

$$\forall n \in \mathbb{Z}, 2n \otimes 1 = n \otimes 2 = 0.$$

So observe:

$$2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \xrightarrow[\varphi]{} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \ ,$$

where we have $\varphi \otimes Id = 0$. Before we had an embedding:

$$0 \longrightarrow 2\mathbb{Z} \xhookrightarrow[\varphi]{} \mathbb{Z} \ ,$$

but it is no longer an embedding when we take the tensor product with $\mathbb{Z}_2$.

We have a similar example:

$$0 \longrightarrow \mathbb{Z} \xhookrightarrow[\varphi]{} \mathbb{Q}$$

EXAMPLE 1.135.

$$0 \longrightarrow \mathbb{Z} \otimes \mathbb{Z}_2 \longrightarrow \mathbb{Q} \otimes \mathbb{Z}_2$$

where taking the tensor product with $\mathbb{Z}_2$, we have $\mathbb{Z} \otimes \mathbb{Z}_2 \cong \mathbb{Z}_2$, but $\mathbb{Q} \otimes \mathbb{Z}_2 = 0$. So it isn't injective.

REMARK 1.136. The tensor product preserves surjectivity, but not injectivity.

LEMMA 1.137. *If:*

$$B \xrightarrow[\psi]{} C \longrightarrow 0$$

is exact (ψ is surjective), then:

$$B \otimes M \xrightarrow[\psi \otimes Id]{} C \otimes M \longrightarrow 0$$

is exact ($\psi \otimes Id$ is surjective).

PROOF. $\forall c \in C, u \in M$, find $b \in B$ s.t. $\psi(b) = c$, then

$$(\psi \otimes Id)(b \otimes u) = c \otimes u.$$

And simple tensors generate $C \otimes M$, so $\psi \otimes Id(B \otimes M) = C \otimes M$. □

THEOREM 1.138. *If:*

$$0 \longrightarrow A \xrightarrow[\varphi]{} B \xrightarrow[\psi]{} C \longrightarrow 0$$

is exact ($\Rightarrow \psi \circ \varphi = 0$, then:

$$A \otimes M \xrightarrow[\varphi \otimes Id]{} B \otimes M \xrightarrow[\psi \otimes Id]{} C \otimes M \longrightarrow 0$$

is exact. (Note that it is still exact on the right, but not on the left, since the zero is dropped)

PROOF. First, $(\psi \otimes Id) \cdot (\varphi \otimes Id) = 0$.

$$(\psi \otimes Id)((\varphi \otimes Id)(a \otimes u)) = (\psi \otimes Id)(\varphi(a) \otimes u) = \psi(\varphi(a)) \otimes u = 0 \otimes u = 0.$$

So we have a hom-sm: $\gamma : B \otimes M/((\psi \otimes Id)(A \otimes M)) \to C \otimes M$. We claim this is an isomorphism, so $ker(\psi \otimes Id) = (\varphi \otimes Id)(A \otimes M)$.

PROOF. Define a hom-sm $C \otimes M \to MB \otimes M/((\psi \otimes Id)(A \otimes M))$ by:

$$c \otimes u \mapsto b \otimes u \mod ((\psi \otimes Id)(A \otimes M)),$$

where b is s.t. $\psi(b) = c$. Why is it well defined? If b' is another element in B s.t. $\psi(b') = c$, then:

$$b' = b \mod \varphi(A),$$

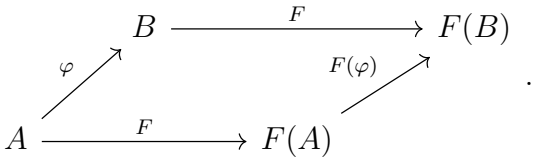
so $b' \otimes u = b \otimes u \mod (\varphi(A) \otimes M)$. So it's well defined. Next we check that it's bilinear, it's obvious. Claim is that this is inverse of γ and it is, we skip the details. □

□

REMARK 1.139. Recall that if we have $\varphi : M \to N$, $K \subseteq M$, and $\varphi(K) = 0$ then we must have a hom-sm $M/K \to N$.

REMARK 1.140. $\otimes M$ is a **functor** from the category of R-modules to itself: $A \Rightarrow A \otimes M$, and $A \to B \Rightarrow A \otimes M \to B \otimes M$.

DEFINITION 1.141. A **functor** from category $\mathcal{C}_1$ to category $\mathcal{C}_2$ is a "mapping" that maps objects to objects and morphisms to morphisms, and preserves compositions of morphisms:



DEFINITION 1.142. A functor is **exact** if it maps short exact sequences to short exact sequences.

REMARK 1.143. $\otimes M$ is a **right-exact** functor (loses exactness at the left term).

DEFINITION 1.144. A functor is **right-exact** if for any short exact sequence:

$$0 \longrightarrow A \xrightarrow[\varphi]{} B \xrightarrow[\psi]{} C \longrightarrow 0 \ ,$$

the sequence:

$$F(A) \xrightarrow[F(\varphi)]{} F(B) \xrightarrow[F(\psi)]{} F(C) \longrightarrow 0$$

is exact.

REMARK 1.145. If R is non-commutative, M is a left R-module, then $\otimes m$ is a functor from category of right R-modules to the category of abelian groups.

There are good modules that preserve exact sequences. They are called flat modules.

DEFINITION 1.146. M is **flat** if whenever:

$$0 \longrightarrow A \xrightarrow[\varphi]{} B$$

is exact, the sequence:

$$0 \longrightarrow A \otimes M \xrightarrow[\varphi \otimes Id]{} B \otimes M$$

is exact. In this case, $\otimes M$ is an exact functor.

Now what modules are flat? The ring R itself is flat.

REMARK 1.147. We state some results concerning flat modules.

(1) R is flat:

$$0 \longrightarrow A \longrightarrow B$$

$\Rightarrow$

$$0 \longrightarrow A \otimes R \xrightarrow[\varphi \otimes Id]{} B \otimes R$$

$=$

$$0 \longrightarrow A \longrightarrow B$$

is exact.

(2) If $M = M_1 \oplus M_2$, then M is flat if and only if both M_1, M_2 are flat.

PROOF. Let $0 \to A \to_\varphi B$ be exact. Then:

$$0 \to A \otimes M \to_{\varphi \otimes Id} B \otimes M$$

is isomorphic to

$$0 \to (A \otimes M_1) \oplus (A \otimes M_2) \to_{\tilde{\varphi}} (B \otimes M_1) \oplus (B \otimes M_2).$$

The things on the left hand side of the $\oplus$ are connected by $\varphi \otimes Id_{M_1}$ and RHS by $\varphi \otimes Id_{M_2}$. And $\tilde{\varphi} = (\varphi_1, \varphi_2)$ and $\tilde{\varphi}$ is injective if and only if φ_1, φ_2 are. $\square$

(3) So R^n (free module of finite rank) is flat. The finiteness is not necessary, it's an exercise in the book.
(4) If M is a direct summand of a free module, i.e. there exists M s.t. $M \oplus N$ is free, then M is flat.
(5) If M_1, M_2 are flat, then $M_1 \otimes M_2$ is flat.

PROOF. $\otimes M_1$ is exact as a functor, and $\otimes M_2$ is exact, so $\otimes(M_1 \otimes M_2) = (\otimes M_1) \otimes M_2$ is exact. So if we have:

$$0 \to A \to B$$

then

$$0 \to A \otimes M_2 \to B \otimes M_2$$

then

$$0 \to A \otimes (M_1 \otimes M_2) \to B \otimes M_1 \otimes M_2.$$

□

(6) If M is flat and I is an ideal in R, then $I \otimes M \to IM$ is an isomorphism. This is standard mapping which maps $a \otimes u \mapsto au$.

PROOF. $0 \to I \to R$ is exact, so:

$$0 \to I \otimes M \to R \otimes M \cong M$$

is exact. And this is a mapping that maps $a \otimes u \mapsto a \otimes u \mapsto au$. So $I \otimes M \to M$ is injective. The inverse of this mapping is just IM. So actually this is an isomorphism of modules. □

(7) Assume R is an integral domain. Then if $Tor(M) \neq 0$, then M is not flat.

PROOF. $0 \to R \to Q$-the field of fractions. □

Thursday, February 1st

LEMMA 1.148. *If R is an integral domain and M is a flat R-module, then $Tor(M) = 0$.*

PROOF. Let Q be the field of fractions of R. Then:

$$0 \to R \to Q$$

is exact. So:

$$0 \to R \otimes M \to Q \otimes M$$

is exact. But $R \otimes M \cong M$ under the isomorphism $\varphi : 1 \otimes u \to u.$, where $ker\varphi = Tor(M)$. So if $u \neq 0$ is in $Tor(M)$, then $1 \otimes u \neq 0 \in R \otimes M$, but is zero in $Q \otimes M$, so $R \otimes M \to Q \otimes M$ is not injective, which is a contradiction since we said the above sequence is exact. □

LEMMA 1.149. *The converse of Lemma 1.148 is not true: if $Tor(M) = 0$, it may not be flat.*

We give a counterexample:

EXAMPLE 1.150. Let $R = F[x, y]$ and let $M = I = (x, y)$. Then M is torsion-free, but:

$$I \otimes M \to IM$$

is not an isomorphism. $x \otimes y - y \otimes x \mapsto 0$. It was one of the properties of flat modules that for any ideal in R, the above map must be an isomorphism, thus M is not flat.

Flatness is related to torsion.

LEMMA 1.151. *If R is an integral domain and Q is its field of quotients, then Q is a flat R-module.*

You can take $S^{-1}R$ for any multiplicatively closed set and this will be a flat R-module.

PROOF. The reason for this is that Q is a union of free R-modules, copies of R. It consists:

$$Q = \bigcup_{d \neq 0} d^{-1}R.$$

Let:

$$0 \to A \to B,$$

be exact. So $\varphi : A \to B$ is injective. Then $(R^*)^{-1}A \cong A \otimes Q \to_{\varphi \otimes Id} B \otimes Q \cong (R^*)^{-1}B$. So we have:

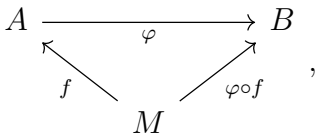
$$\varphi \otimes Id(\frac{u}{r} = \frac{\varphi(u)}{r}, u \in A, r \in R.$$

And $\frac{\varphi(u)}{r} = 0$ if and only if $a\varphi(u) = 0$ for some $a \neq 0$. Then $\varphi(au) = 0$, and since φ is injective, $au = 0$, so $\frac{u}{r} = 0$ is in $(R)^*)^{-1}A$. So $\varphi \otimes Id$ is injective. □

Refer to Remarks 1.126,1.127. For equivalent definitions of exactness.
We discuss **projective and injective modules.**

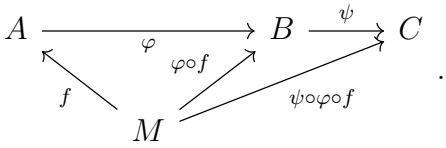
DEFINITION 1.152. Let R be commutative unital. Let M be an R-module.
Functors: $Hom_R(m, \cdot)$ and $Hom_R(\cdot, M)$.
For any R-module A, we have new modules $Hom_R(M, A)$ and $Hom_R(A, M)$.

If $\varphi : A \to B$ is a hom-sm, then we have a hom-sm $Hom(M, A) \to Hom(M, B)$. How is it defined? We have:



,

so $f \to \varphi \circ f$. And if we have one more module, we have:



.

So:

$$\begin{aligned} Hom(M, A) \to Hom(M, B) \to Hom(M, C) \\ f \mapsto \varphi \circ f \mapsto \psi(\varphi \circ f) = (\psi \circ \varphi) \circ f. \end{aligned} \tag{1.45}$$

THEOREM 1.153. *If $0 \to A \to B \to C \to 0$ is exact, then:*

$$0 \to Hom(M, A) \xrightarrow{\tilde{\varphi}} Hom(M, B) \xrightarrow{\tilde{\psi}} Hom(M, C)$$

is exact, i.e. the functor $Hom(M, \cdot)$ is left exact, but not exact, since exactness is not preserved on the right.

PROOF. We have:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \longrightarrow & 0 \\ & & & \nwarrow^{f} & \uparrow{\scriptstyle \varphi\circ f} & & & & \\ & & & & M & & & & \end{array} .$$

Assume that $\varphi \circ f = 0$. φ is injective by definition of exactness. And we have $\varphi(f(a)) = 0, \forall u \in M$, so $f(u) = 0, \forall u \in M$, since φ is injective, so $f = 0$. Thus we have proved that $\tilde{\varphi}$ is injective..

Now consider $f \in Hom(M, A) \mapsto \varphi \circ f \in Hom(M, B) \mapsto \psi \circ \varphi \circ f \in Hom(M, C)$. And $\psi \circ \varphi \circ f = 0$ since $\psi \circ \varphi = 0$ by exactness. So $Image(\tilde{\varphi}) \subseteq ker(\tilde{\psi})$. Now let $g \in ker(\tilde{\psi})$, that is, $\psi \circ g = 0$. Then:

$$\psi|_{g(M)} = 0.$$

So $g(M) \subseteq ker\psi$, so $g(M) \subseteq \varphi(A)$. Then we have $f : M \to A$ defined by $f(u) = \varphi^{-1}(g(u))$. So $g = \varphi \circ f = \varphi^{-1}(f)$. The inverse is well defined since φ is injective. □

We give counterexample to show that it is not exact on the right.

Example 1.154. Let $M = \mathbb{Z}_2$. Note $\mathbb{Z} \to \mathbb{Z}_2 \to 0$ is exact, we have a map $h : \mathbb{Z}_2 \to \mathbb{Z}_2$, the identity map, but there's no map g from $\mathbb{Z}_2$ to $\mathbb{Z}$ s.t. $h = \psi \circ g$, where ψ is the map from $\mathbb{Z} to \mathbb{Z}_2$.

Definition 1.155. M is **projective** if $Hom(M, \cdot)$ is exact: $\forall$ surjective $\psi : B \to C$ and $h : M \to C$ there exists $g : M \to B$ s.t. $h = \psi \circ g$:

$$\begin{array}{ccccc} B & \longrightarrow & C & \longrightarrow & 0 \\ & \nwarrow^{g} & \uparrow{\scriptstyle h} & & \\ & & M & & \end{array} .$$

So we know $Hom(M, B) \to Hom(M, C) \to 0$ is exact.

Remark 1.156. We list some properties of projective R-modules.

(1) If $M = M_1 \oplus M_2$, then M is projective if and only if M_1 and M_2 are. Proof is easy apparently.
(2) R, R^n are projective, and any free module is projective. This follows from the first property for free modules of finite rank.

    Proof. Take $e_i \to c_i$. Find $b_i \in B$ s.t $\psi(b_i) = c_i$ for all i, and define $g(e_i) = b_i$. Done. □
(3) If M is a direct summand of a projective module, then it is projective. This is just a reformulation of the first property. And this is a criterion.

Theorem 1.157. *M is projective if and only if M is a direct summand of a free module: $\exists N$ s.t. $M \oplus N$ is free.*

Friday, February 2nd

Definition 1.158. Recall that M is **projective** if $\forall$ exact $B \xrightarrow{\varphi} C \to 0$ and $h : M \to C$ there exists $g : M \to B$ s.t. $h = \varphi \circ g$:

$$\begin{array}{ccccc} B & \longrightarrow & C & \longrightarrow & 0 \\ & \nwarrow^{g} & \uparrow{\scriptstyle h} & & \\ & & M & & \end{array} .$$

DEFINITION 1.159. $Hom(M, \cdot)$ is an **exact functor:** if $0 \to A \to B \to C \to 0$ is exact, then $0 \to Hom(M, A) \to Hom(M, B) \to Hom(M, C) \to 0$ is exact. (Equivalent defn to above).

REMARK 1.160. If M is projective and $B \xrightarrow{\varphi}$ is surjective then $\exists$ a section of $\varphi : s : M \to B$ s.t. $\varphi \circ s = Id_M$. Indeed, we have:

$$\begin{array}{ccccc} B & \xrightarrow{\varphi} & M & \longrightarrow & 0 \\ & \nwarrow^{s} & \uparrow{\scriptstyle Id_M} & & \\ & & M & & \end{array}$$

so there exists s s.t. $\varphi \circ s = Id_M$. Recall that a section is a map from $M \to B$ s.t. it maps the image of an element from surjective hom-sm back to the same element.

REMARK 1.161. If M is projective, then any short exact sequence $0 \to A \to B \to M \to 0$ splits s.t. $B \cong A \oplus M$.

In particular, since M is a quotient of a free module $F \to M \to 0$, if M is projective, then M is a direct summand of a free module, since we have a section from $M \to F$ that makes it a direct summand. Conversely, if M is a direct summand of a free module, it is projective: $F = M \oplus N$.

DEFINITION 1.162. $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ splits "from the left" if $\exists \pi : B \to A$ s.t. $\pi \circ \varphi = Id_A$.

PROOF. Let $C' = ker\pi$. We claim $\psi|_{C'}$ is isomorphic $C' \cong C$. Indeed ψ is surjective (because short exact), and if $b \in C'$ and $\psi(b) = 0$. Then $ker\psi = \varphi(A)$, by short exact, so if $b \in ker\psi$, then $b = \varphi(a)$ for some $a \in A$. Then $\pi(b) = a$ by definition of section. But if $b \in C'$, $\pi(b) = 0$, so $a = 0$, so $b = 0$. So we proved that $b \in ker\pi \Rightarrow b = 0$. So π is injective. Now we claim that $\varphi(A) + C' = B$. So since φ is a bijection, we know $\varphi(A) \cong A$.

PROOF. Let $b \in B$, let $a = \pi(b)$. Then $b - \varphi(a) \in C'$, since $\pi(b - \varphi(a)) = a - a = 0$. So $b \in \varphi(A) + C'$. □

Now claim $C' \cap \varphi(A) = 0$. If $b \in C'$, then $\pi(b) = 0$, and if $b = \varphi(a)$, then $\pi(b) = \pi(\varphi(a)) = a = 0$, so $b = 0$. More work to be done here. □

We discuss injective modules. Which is related to $Hom(\cdot, M)$. Fix M. Let's consider this functor. You have module $A \Rightarrow$ module $Hom(A, M)$. If you have $A \xrightarrow{\varphi} B$, then you have $Hom(B, M) \xrightarrow{\tilde{\varphi}} Hom(A, M)$.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & M & \end{array}$$

$f = g \circ \varphi$. We have $\tilde{\varphi} = g \circ \varphi$. This is a **contravariant functor** - it inverts arrows (morphisms). What we had before was called a **covariant** functors ("normal" ones).

DEFINITION 1.163. **Covariant:** $A \Rightarrow F(A)$:

$$A \to B \Rightarrow F(A) \to F(B).$$

DEFINITION 1.164. **Contravariant:** $A \Rightarrow F(A)$:

$$A \to B \Rightarrow F(B) \to F(A).$$

Note $F(B)$ is first here on the right side.

THEOREM 1.165. *$Hom(\cdot, M)$ is left exact: if $0 \to A \to B \to C \to 0$ is exact, then $0 \to Hom(C, M) \to Hom(B, M) \to Hom(A, M)$ is exact.*

PROOF. Left as an exercise to the reader, it is straightforward. (wtf) □

It may not be exact, tho. If $0 \to A \xrightarrow{\varphi} B$ is exact (φ is injective):

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & B \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle g} & \\ & & M & & \end{array}$$

and we have $f : A \to M$ we need $g : B \to M$ s.t. $f = g \circ \varphi$. We give a counterexample:

EXAMPLE 1.166. Consider:

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 2} & \mathbb{Z} \\ & & \downarrow{\scriptstyle Id} & \swarrow{\scriptstyle g} & \\ & & \mathbb{Z} & & \end{array}$$

Note $2\mathbb{Z} \subseteq \mathbb{Z}$ but we have no such g. We have no map going from $2n \to n$.

DEFINITION 1.167. M is **injective** if $\forall 0 \to A \xrightarrow{\varphi} B$ (exact) and $\forall f : A \to M$ there exists $g : B \to M$ s.t. $f = g \circ \varphi$.

REMARK 1.168. M is injective if and only if $Hom(\cdot, M)$ is an exact functor.

REMARK 1.169.
(1) $M = M_1 \oplus M_2$ is injective if and only if both M_1 and M_2 are injective.
(2) R is not injective, generally speaking. ($\mathbb{Z}$ is not injective $\mathbb{Z}$-module)
(3) Q is an injective $\mathbb{Z}$-module.

LEMMA 1.170. *Any module is a quotient of a free module, so, of a projective module.*

THEOREM 1.171. *Any module is a submodule of an injective module.*

Monday, February 5th

DEFINITION 1.172. A module M is **divisible** if $\forall$ nonzero divisor $a \in R$, $\forall u \in M$, there is a $v \in M$ s.t. $av = u$. That is, $M \to M$, where $v \mapsto av$ is surjective. So if R is an integral domain it is always true?

REMARK 1.173. If M is injective, then M is divisible.

REMARK 1.174. Let R be an integral domain, if M is divisible, and either M is torsion free or R is a PID, then M is injective.

LEMMA 1.175 (**Baer's criterion**). *M is injective if $\forall$ ideal I of R, $\forall f : I \to M$ there exists $g : R \to M$ s.t $g|_I = f$. So this proves that the field of fractions is injective.*

REMARK 1.176. M is projective if and only if: if M is a quotient module of some module B, $B \to M \to 0$, then we have $B \cong N \oplus M$. And in fact we have $0 \to N \to B \to M \to 0$.

REMARK 1.177. Injective if and only if $0 \to M \to B$ implies $B \cong N \oplus M$. $M \subseteq B$. Then there exists $N \subseteq B$ s.t. the above is true. So M is injective if and only if if M is a submodule of B then M is a direct summand of B.

REMARK 1.178. $\prod^{\infty} \mathbb{Q} \cong \bigoplus_{\alpha \in \Lambda} \mathbb{Q}$. This is only because on the left, that is a vector space. And thus it has a basis.

LEMMA 1.179. *$M = \prod_{i=1}^{\infty} \mathbb{Z}$ is not free.*

PROOF. Let $N = \bigoplus_{I=1}^{\infty} \mathbb{Z} \subseteq M$. Assume that M is free, let B be a basis. There exists $B' \subseteq B$ which is countable s.t. $N \subseteq N' = \mathbb{Z}B'$. For $u \in N$, let$B_u \subseteq B$ finite be s.t. $u \in RB_u$. Then:

$$B' = \cup_{u \in N} B_u.$$

which is countable. Let $\tilde{M} = M/N'$ a free module, $\cong R(B/B')$. Note B is uncountable. If K is a free $\mathbb{Z}$-module, then K is not divisible: $\forall v \in K$, $v = (0, ..., n_i, ..., n_j, 0, ...)$ v is only divisible by $\gcd(N_i, ..., n_j)$. So no element of k is divisible if it is nonzero. Recall that v is divisible if and only if $\forall k \neq 0$, there exists w s.t. $kw = v$. We claim $\tilde{M}$ has divisible elements, so we have contradiction. Take:

$$u = (\pm 1, \pm 2!, \pm 3!, \pm 4!, ...) \in M,$$

In $\tilde{M}$, $N = 0$, so take:

$$\overline{u} = (0, 0, ..., 0, k!, (k+1)!, ...) \in \tilde{M},$$

which is divisible by k for all k. We have uncountably many of such u, not all of them are in N', so there exists such u with $\overline{u} \neq 0$ in $\tilde{M}$. □

10.5 Exercises

1. *Suppose that:*

$$\begin{array}{ccccc} A & \xrightarrow{\psi} & B & \xrightarrow{\varphi} & C \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ A' & \xrightarrow{\psi'} & B' & \xrightarrow{\varphi'} & C' \end{array}$$

is a commutative diagram of groups and that the rows are exact. Prove that:

(a) *If φ and α are surjective, and β is injective then γ is injective.*

PROOF. Let $c \in ker\gamma$. Then we know there exists $b \in B$ s.t. $\varphi(b) = c$, since φ is surjective. Note that $\varphi'(\beta(b)) = \gamma(\varphi(b)) = \gamma(c) = 0$ since it is a commutative diagram. So we know $\beta(b) \in ker\varphi' = \psi'(A')$ since the bottom row is exact, so we know there exists $a' \in A'$ s.t. $\psi'(a') = \beta(b)$. And since α is surjective, we know there exists $a \in A$ s.t. $\alpha(a) = a'$. Then since $\psi'(\alpha(a)) = \beta(b)$, and the diagram is commutative, we know we must have $\beta(\psi(a)) = \psi'(\alpha(a)) = \beta(b)$. Now since β is injective, we know $b = \psi(a)$. But recall that $c = \varphi(b) = \varphi(\psi(a)) = 0$ since the top row is exact. Thus since $ker\gamma = 0 \in C$, we know that γ is injective. □

(b) *If ψ', α, and γ are injective, then β is injective.*

PROOF. Let $\beta(b) = 0$ for some $b \in B$. Then we have $\varphi'(\beta(b)) = 0 = \gamma(\varphi(b))$ by commutativity. Since γ is injective, we know $\varphi(b) = 0$, so $b \in \psi(A)$. So there exists $a \in A$ s.t. $\psi(a) = b$. Now note that since we have commutativity

we know $\beta(\psi(a)) = 0 = \psi'(\alpha(a))$. But since α and ψ' are both injective, we know $a = 0$, hence $\psi(a) = b = 0$, and β is injective. □

(c) *If φ, α and γ are surjective, then β is surjective.*

PROOF. Let $b' \in B$. Then $\varphi'(b') \in C'$. So there exists $c \in C$ s.t. $\gamma(c) = \varphi'(b')$ since γ is surjective and there exists $b \in B$ s.t. $\varphi(b) = c$ since φ is surjective. So we know $\gamma(\varphi(b)) = \varphi'(\beta(b)) = \varphi'(b')$. So $\varphi'(\beta(b) - b') = 0$, so $\beta(b) - b' \in ker\varphi' = \psi'(A')$. So we know there exists $a' \in A'$ s.t. $\psi'(a') = \beta(b) - b'$. But since α is surjective and $a' \in A'$, we know there exists $a \in A$ s.t. $\psi'(\alpha(a)) = \psi'(a') = \beta(b) - b'$. So we must have that $\beta(\psi(a)) = \beta(b) - b'$ by commutativity. For $b - \psi(a)$ we then have $\beta(b - \psi(a)) = \beta(b) - \beta(b) + b' = b'$, which proves that β is surjective. □

(d) *If β is injective, α and φ are surjective, then γ is injective.*

PROOF. Let $c \in C$ s.t. $\gamma(c) = 0$. Then since φ is surjective we have $b \in B$ s.t. $\varphi(b) = c$. Now take $\psi'(\beta(b)) = 0$ by commutativity since $\gamma(\varphi(b)) = 0$. Then we know $\beta(b) \in ker\varphi' = \psi'(A)$ so we have $a' \in A'$ s.t. $\psi'(a') = \beta(b)$. And since α is surjective we have $a \in A$ s.t. $\alpha(a) = a'$. So we have $\psi'(\alpha(a)) = \beta(b) = \beta(\psi(a))$ by commutativity. But since β is injective we know $\psi(a) = b$ But then $b \in \varphi(A) = ker\varphi$ so $\varphi(b) = 0 = c$. So γ is injective. □

(e) *If β is surjective, γ and ψ' are injective, then α is surjective.*

PROOF. Let $a' \in A$. Then $\varphi'(\psi'(a)) = 0 \in C'$. Also since β is surjective we have $b \in B$ s.t. $\beta(b) = \psi'(a')$. Now $\gamma(\varphi(b)) = \varphi'(\beta(b))$ by commutativity, but $\varphi'(\beta(b)) = \varphi'(\psi'(a')) = 0$, so $\gamma(\varphi(b)) = 0$, and since γ is injective, $\varphi(b) = 0$. Thus by exactness, we have $a \in A$ s.t. $\psi(a) = b$. Now take $\psi'(\alpha(a)) = \beta(\psi(a)) = \psi'(a')$, and by injectivity of ψ', we know $\alpha(a) = a'$. So α is surjective. □