Contents

Chapter 1

Information and Disclaimers

Information. These are class notes for the second year graduate level algebra course at UNL (Math 902) as taken in class and later typed by Kat Shultis. The notes are from the Spring of 2012, and that semester the course was taught by Tom Marley. During the fall semester we covered the following topics:

▷ Ring Theory: Noetherian/Artinian, Semisimple, Simple, Artin-Wedderburn Theory
▷ Representation Theory: Representations of Group Rings, Characters
▷ Commutative Algebra: Localization, Tensor Products, Projective and Injective Modules

For each class day, I've indicated the topic at the top of that day's notes.

Disclaimer. I created these notes in order to help me study, and so I've expanded proofs where I find it useful, shortened things I was comfortable with before this course, and changed at least one proof to one that I like better than the one presented in class. These notes are not meant to be a substitute for your own notes. They have been proof-read, but are not guaranteed to be without errors. If you find errors, please email Kat at the following address:

`s-kshulti1` "at" `math.unl.edu`

Notation. I'm tired of deciding whether or not $0 \in \mathbb{N}$ and so I've adopted the following for notational ease. For any $n \in \mathbb{Z}$, set $\mathbb{N}_n := \{a \in \mathbb{Z} \mid a \geq n\}$. So, $0 \in \mathbb{N}_0$, but $0 \notin \mathbb{N}_1$.

Chapter 2

Exam 1 Material

2.1 Monday 9 January 2012

2.1.1 Examples of Non-Commutative Rings

Comment. In this class, all rings will have a multiplicative identity.

Example 1. Here we'll give a few examples of how to construct non-commutative rings.

1. Matrix Rings: Let R be any ring. Let $M_n(R) = \{n \times n \text{ matrices with entries in } R\}$. Then $M_n(R)$ is a *non-commutative* ring for $n \geq 2$.
2. Endomorphism Rings: Let R be a commutative ring, and M an $R-$module. Then
$$\text{End}_R(M) = \{f : M \to M | f \text{ is } R - \text{linear}\}$$
is a ring under addition and function composition. It is typically *non-commutative*.
3. Group Rings: Let G be a group. Let R be a commutative ring, and let $R[G]$ be the free $R-$module with basis $\{g|g \in G\}$. That is, every element in $R[G]$ is written uniquely as $r_1g_1 + \ldots + r_ng_n$ with $r_i \in R$ and $g_i \in G$. The multiplication to make this a ring is $\left(\sum_{g\in G} r_g g\right)\left(\sum_{h\in G} s_h h\right) = \sum_{g,h\in G} r_g s_h gh$. In particular, if $G =< a \mid a^2 = 1 >$, and $R = k$ is a field, then $k[G] = \{r_0 + r_1 a \mid r_0, r_1 \in k\}$. Note here that $R[G]$ is *non-commutative* if and only if G is non-abelian.
4. Skew-Polynomial Rings: Let R be a commutative ring. Let $\sigma : R \to R$ be a ring homomorphism, and let $R[x;\sigma]$ be the $R-$module $R[x]$. That is, every element has the form $a_nx^n + \ldots + a_1x + a_0$, with $a_i \in R$. Here, the multiplication is given as follows for monomials, and extended linearly: $a_nx^n \cdot b_mx^m = a_n\sigma^n(b_m)x^{n+m}$. Note here that if σ is the identity homomorphism, then this is just $R[x]$. Also, $R[x;\sigma]$ is *non-commutative* when σ is not the identity.

2.1.2 Noetherian & Artinian Modules

Definition 2. Let R be a ring, and M a left $R-$module. Then M is called *Noetherian (resp. Artinian)* if M satisfies ACC (resp. DCC) on left submodules. Recall here what ACC and DCC say: ACC (resp. DCC) is if given any ascending (resp. descending) chain $N_0 \subseteq N_1 \subseteq \ldots$ (resp. $N_0 \supseteq N_1 \supseteq \ldots$) of submodules of M, there exists a $k \in \mathbb{N}$ such that $N_k = N_{k+i}$ for all $i \geq 0$.

Proposition 3. *Let R be a ring, and M a left $R-$module. TFAE:*

a. M is Noetherian (resp. Artinian),
b. every non-empty set of submodules of M has a maximal (resp. minimal) element,

In the Noetherian case, we also have:

c. every submodule of M is finitely generated.

Proof. We'll only do the proof in the Noetherian case, but the Artinian case proof follows mutatis mutandis[1].
(a. $\Rightarrow$ b.) Let Λ be a nonempty set of submodules of M. Let $M_1 \in \Lambda$. By way of contradiction, assume Λ does not have a maximal element. Then there exists some $M_2 \in \Lambda$ so that $M_1 \subsetneq M_2$. This process can be continued, that is, we can find some $M_3 \in \Lambda$ so that $M_2 \subsetneq M_3$, etc. This gives a violation of ACC, so we have a contradiction, and that completes this part of the proof.
(b. $\Rightarrow$ c.) Let N be a submodule of M and let $\Lambda = \{\text{finitely generated submodules of } N\}$. Note that $0 \in \Lambda$ so that Λ is non-empty. By assumption, then Λ has a maximal element, say N'. If $N' \subsetneq N$, then there is some $x \in N \setminus N'$, and we can set $N'' = N' + Rx$, so that N'' is finitely generated, and $N'' \supsetneq N'$. This is a contradiction as $N'' \in \Lambda$ but N' was maximal. Hence $N' = N$, so that $N \in \Lambda$, and N is finitely generated.
(c. $\Rightarrow$ a.) Let $N_0 \subseteq N_1 \subseteq \ldots$ be an ascending chain of submodules of M, and set $N = \bigcup_{i=0}^{\infty} N_i$. Note that N is a

[1] See Hungerford page xv. This is latin for (roughly) "by changing the things which (obviously) must be changed (in order that the argument will carry over and make sense in the present situation)."

submodule of M since the submodules are nested, and so N is finitely generated. Say $N = Rx_1 + \ldots + Rx_\ell$ and choose t so that $x_i \in N_t$ for all i. Then $N_t \subseteq N \subseteq N_t$ so that $N = N_t = N_{t+j}$ for all $j \geq 0$. Hence, the chain terminates and this completes the proof. □

Comment. Let $R = k$ be a field. Then every $R-$module is a $k-$vector space, so that any $k-$vector space V is Noetherian if and only if it is Artinian which in turn is true if and only if $\dim_k V < \infty$. Similarly, if R is a division ring, then every left $R-$module has a basis, and a well defined notion of dimension and we again get that Noetherian, Artinian and finite dimensional are all equivalent for vector spaces over division rings.

Example 4. Let $R = k[x]$ where k is a field. Then R is Noetherian but not Artinian. The non Artinian part can be seen with the following descending chain $(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \ldots$.

Example 5. Let $M = \left\{ \frac{a}{2^n} | a \in \mathbb{Z}, n \geq 0 \right\}$, and consider M as a $\mathbb{Z}-$module. Note here that $\mathbb{Z} \subseteq M \subseteq \mathbb{Q}$. Also, let $T = M/\mathbb{Z}$. Then T is Artinian but not Noetherian. We'll show this, and for notational purposes, let $\overline{\frac{a}{2^n}}$ denote $\frac{a}{2^n} + \mathbb{Z}$. For $n \geq 0$ let $N_n = \mathbb{Z} \cdot \overline{\frac{1}{2^n}}$ and notice that $N_n \subseteq T$.

First, we show that $N_n \subsetneq N_{n+1}$ which shows that T is not Noetherian as it provides an ascending chain that doesn't stabilize. Since $\overline{\frac{1}{2^n}} = 2 \cdot \overline{\frac{1}{2^{n+1}}}$, then for any $a \in \mathbb{Z}$, we have $a \cdot \overline{\frac{1}{2^n}} = 2a \cdot \overline{\frac{1}{2^{n+1}}}$ which gives the containment. To show the containment is strict, suppose that $\overline{\frac{1}{2^{n+1}}} = a \cdot \overline{\frac{1}{2^n}}$ for some $a \in \mathbb{Z}$. Then we get $\frac{1}{2^{n+1}} - \frac{a}{2^n} \in \mathbb{Z}$ but that $\frac{1}{2^{n+1}} - \frac{a}{2^n} = \frac{1-2a}{2^{n+1}} \notin \mathbb{Z}$ so we have a contradiction, and hence the containment is strict.

Now, we claim that every proper $\mathbb{Z}-$submodule of T is N_n for some n. If we can show this, then any descending chain of submodules of T must start with N_n for some n, and the only submodules of N_n are N_i where $0 \leq i < n$ and so the chain will stabilize, and we'll get that T is Artinian. So let $A \subsetneq T$ be a proper submodule. Choose n to be the largest integer so that $\overline{\frac{1}{2^n}} \in A$. Such an element exists as A is a proper submodule, and $\overline{\frac{1}{2^0}} \in A$. So we claim that $A = N_n$. We clearly have that $N_n \subseteq A$, so let $\overline{\frac{a}{2^m}} \in A$ and suppose that $\overline{\frac{a}{2^m}} \notin N_n$. Without loss of generality, we may assume that a is odd, and we also have that $m \geq n+1$. Since $gcd(a, 2^m) = 1$, then there exist integers x, y so that $ax + 2^m y = 1$. Hence, $x\frac{a}{2^m} + y = \frac{1}{2^m}$. Modding out by $\mathbb{Z}$ gives $x \cdot \overline{\frac{a}{2^m}} = \overline{\frac{1}{2^m}}$ and since $\overline{\frac{a}{2^m}} \in A$ this gives that $\overline{\frac{1}{2^m}} \in A$. This is a contradiction as $m \geq n+1$ and n was chosen to be maximal. Hence, $A = N_n$.[2]

2.2 Wednesday 11 January 2012

2.2.1 Exact Sequences

Definition 6. A sequence of left $R-$modules and $R-$homomorphisms

$$\cdots \longrightarrow N_{i-1} \xrightarrow{f_{i-1}} N_i \xrightarrow{f_i} N_{i+1} \longrightarrow \cdots$$

is *exact* if $\text{image}(f_{i-1}) = \ker(f_i)$ for all i.

Definition 7. An exact sequence is a *Short Exact Sequence (SES)* if it is of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0. \tag{2.1}$$

Equivalently, this is if f is injective, g is surjective, and $\text{image}(f) = \ker(g)$.

Comment. Let N be a submodule of M. Then the following sequence is always exact where i and π are the usual inclusion and projection maps:

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0.$$

[2] We did most of this example on Wednesday, but we at least tried to start it today, and it fits better here.

In fact, if one considers any SES, it has this form (up to isomorphism). This is because (using the generic notation from the SES in 2.1) we have that f is an injection so that $A \cong f(A) \subseteq B$. Similarly, as g is a surjection, then by the first isomorphism theorem we have $C = \text{image}(g) \cong B/\ker(g) = B/f(A)$.

Example 8. The sequence below is a short exact sequence. Note that the map from $\mathbb{Z}$ to $\mathbb{Z}$ is being given by multiplication by 2.

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Definition 9. Let M_1, M_2 be $R-$modules and note that the following is a SES:

$$0 \longrightarrow M_1 \xrightarrow{f} M_1 \oplus M_2 \xrightarrow{g} M_2 \longrightarrow 0.$$

where $f(m_1) = (m_1, 0)$ and $g(m_1, m_2) = m_2$. A short exact sequence of this form is called *split exact*.

Proposition 10. *Let R be a ring and*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0.$$

a SES of left $R-$modules. Then B is Noetherian (resp. Artinian) if and only if both A and C are Noetherian (resp. Artinian).

Proof. We'll only show this in the Artinian case, but the Noetherian case follows mutatis mutandis. Also, without loss of generality, we'll assume that A is a submodule of B and that $C = B/A$.
($\Rightarrow$) Let B be Artinian, and let $N_0 \supseteq N_1 \supseteq \dots$ be a descending chain of submodules of A. Then this is also a descending chain of submodules of B since $A \subseteq B$ and all submodules of A are also submodules of B. Hence the chain terminantes and A is Artinian.
Next, let B be Artinian, and let $N_0 \supseteq N_1 \supseteq \dots$ be a descending chain of submodules of C. Then for all i we have $N_i = B_i/A$ where B_i is a submodule of B. We then have that $B_0 \supseteq B_1 \supseteq \dots$ is a descending chain of submodules of B and so there is some $n \in \mathbb{N}$ such that $B_n = B_{n+i}$ for all $i \geq 0$. Thus, $N_n = B_n/A = B_{n+i}/A = N_{n+i}$ for all i and so C is Artinian as well.[3]
($\Leftarrow$) Suppose that A and B/A are Artinian. Let $N_1 \supseteq N_2 \supseteq \dots$ be a descending chain in B. Then $N_1 \cap A \supseteq N_2 \cap A \supseteq \dots$ is a descending chain in A and A is Artinian, and so there exists a $k \in \mathbb{N}$ so that $N_k \cap A = N_{k+i} \cap A$ for $i \geq 0$. Also, $\dfrac{N_1 + A}{A} \supseteq \dfrac{N_2 + A}{A} \supseteq \dots$ is a descending chain in B/A and B/A is Artinian, and so there exists an $\ell \in \mathbb{N}$ so that $\dfrac{N_\ell + A}{A} = \dfrac{N_{\ell+i} + A}{A}$ for $i \geq 0$. Let $t = \max(k, \ell)$. Then we claim that $N_t = N_{t+i}$ for $i \geq 0$. To show this it is sufficient (by induction) to show that $N_t \subseteq N_{t+1}$. So let $n \in N_t \subseteq N_t + A = N_{t+1} + A$ and note that this last equality is due to the correspondence theorem, and the fact that $t \geq \ell$. Then $n = n' + a$ where $n' \in N_{t+1}$ and $a \in A$. Then, we get $n - n' \in A \cap N_t = A \cap N_{t+1} \subseteq N_{t+1}$, and since $n' \in N_{t+1}$ this gives that $n \in N_{t+1}$ as well. □

Corollary 11. *Let $M_1, \dots, M_n$ be $R-$modules. Then $\oplus_{i=1}^n M_i$ is Noetherian (resp. Artinian) if and only if every M_i is Noetherian (resp. Artinian).*

Proof. The proof of this follows from the proposition applied to a split exact sequence and induction. □

2.2.2 Noetherian & Artinian Rings

Definition 12. Let R be a ring. Then R is both a left and a right $R-$module. Note that the left (resp. right) submodules of R are *left (resp. right) ideals*. We say R is *left (resp. right) Noetherian (resp. Artinian)* if it is Noetherian (resp. Artinian) as a left (resp. right) $R-$module.

Proposition 13. *Let R be a left Noetherian (resp. Artinian) ring. Then every finitely generated left $R-$module is Noetherian (resp. Artinian).*

Proof. We'll only show this in the Artinian case, but the proof for Noetherian follows mutatis mutandis. Let R be a left Artinian ring. Then R^n is a left Artinian $R-$module for all n. If M is a finitely generated left $R-$module, then there is some $n \in \mathbb{N}$ and some module homomorphism $\varphi : R^n \to M$ so that φ is surjective. Thus, $M \cong R^n/\ker\varphi$. Since quotients of left Artinian modules are also Artinian, then M is Artinian. □

[3] In class we said this direction is trivial, but I feel it is worth stating the actual argument.

2.3 Friday 13 January 2012

2.3.1 Noetherian & Artinian Rings

Definition 14. Let R be a ring. R is *Noetherian (resp. Artinian)* if it is both left and right Noetherian (resp. Artinian).

Remark 15. Let $\phi : R \to S$ be a ring homomorphism. Then S is a left $R-$module via $r \cdot s = \phi(r)s$. So every left $S-$module is also a left $R-$module. Suppose S is finitely generated as a left $R-$module. That is, $S = Ru_1 + \ldots + Ru_t$ for some $u_1, \ldots, u_t \in S$. If R is left Noetherian (resp. Artinian) as a ring, then S is left Noetherian (resp. Artinian) as a ring. This is because as S is finitely generated as a left $R-$module, then S is Noetherian as a left $R-$module.

Example 16. 1. Consider the ring homomorphism $\phi : R \to M_n(R)$ given by $r \longmapsto rI_n$, and let E_{ij} be the matrix with 1 in the i, j entry and 0 elsewhere. Then $M_n(R)$ is generated as an $R-$module (left or right) by the E_{ij}'s. That is, $M_n(R) = \sum_{i,j} RE_{ij} = \sum_{i,j} E_{ij}R$. Thus, if R is left Noetherian (resp. Artinian), so is $M_n(R)$. Here, a special case is that if D is a division ring, then $M_n(D)$ is both Noetherian and Artinian.
2. Let G be a group, and R a ring. Consider $\phi : R \to R[G]$ where $R[G] = \oplus_{g\in G} Rg = \oplus_{g\in G} gR$, and the map is given by $r \longmapsto re_G$. If $|G| < \infty$, then $R[G]$ is a finitely generated $R-$module (on either side), so if R is left Noetherian (resp. Artinian), so is $R[G]$. Here, a special case is that if F is a field, and $|G| < \infty$, then $F[G]$ is both Noetherian and Artinian.

Comment. Many times we'll only say something on the left, but it is also true on the right.

Theorem 17 (Hilbert Basis Theorem). *Let R be a left Noetherian ring, and x and indeterminate. Then $R[x]$ is also left Noetherian.*

Remark 18. Subrings of Artinian (or Noetherian) rings are not necessarily Artinian (or Noetherian).

Example 19. 1. We have $\mathbb{Z} \subseteq \mathbb{Q}$ and $\mathbb{Q}$ is both Noetherian and Artinian, but $\mathbb{Z}$ is not Artinian.
2. We can adjoin infinitely many indeterminants to get $k[x_1, \ldots] \subseteq k(x_1, \ldots)$ where k is a field and $k(x_1, \ldots)$ is Noetherian but $k[x_1, \ldots]$ is not Noetherian.
3. If k is a field then $R = k[x, y]$ is Noetherian and contains $S = k[x, xy, xy^2, xy^3, \ldots]$ but S is not Noetherian.

Example 20. Let R be a ring, and $S = M_n(R)$. For $k \in \{1, \ldots, n\}$ let $I_k = \{[a_{ij}] \in S \mid a_{ij} = 0 \text{ whenever } j \neq k\}$. These are columns in the matrices. Then I_k is a left ideal, but not a right ideal for $n \geq 1$.

Comment. If I is a left ideal of R, then R/I is a left $R-$module, but it is not necessarily a ring (unless I is a $2-$sided ideal). An *ideal* of R is a left ideal which is also a right ideal. If I is an ideal, then R/I is a ring. Also, (0) and R are the trivial ideals.

2.3.2 Simple Rings

Definition 21. A ring R is called *simple* if it has no nontrivial ideals.

Comment. 1. If R is a commutative ring, then R is simple if and only if it is a field.
2. Division rings are simple.
3. There exist simple rings which aren't division rings (and even ones that aren't left or right Artinian)!

Example 22. Let F be a field, and $\sigma : F \to F$ a non-zero ring homomorphism which is **not** surjective, and consider $R = F[x; \sigma]$. Recall that this means we set $x \cdot a = \sigma(a)x$ for $a \in F$. Then R is left Noetherian but not right Noetherian.

Proof. We can use the Euclidean algorithm on $R = F[x; \sigma]$. That is, for $f, g \in R$ with $g \neq 0$, there exist $q, r \in R$ such that $f = qg + r$ and $\deg(r) < \deg(g)$. If $I \neq (0)$ is a left ideal of R, then choose $g \in I \setminus \{0\}$ of smallest degree. Then $I = Rg$, which means that every left ideal of R is finitely generated, and hence R is left Noetherian.
It remains to show that R is not right Noetherian. So choose $b \in F \setminus \sigma(F)$. Then for all $n \geq 1$ we claim that $x^n bx \notin x^{n-1}bxR + \ldots + x^0 bxR$. This will give an infinite properly ascending chain of right ideals. We show this by contradiction. So suppose that $x^n bx = x^{n-1}bxf_{n-1}(x) + \ldots + bxf_0(x)$ with $f_0(x) \in R$. Then we get by rearranging things that $bxf_0(x) = xg(x)$ for some $g(x) \in R$ as all the other terms start on the left with an x. So we have $f_0(x) = c_r x^r + \ldots + c_0$ and $g(x) = a_r x^r + \ldots + a_0$ since both $f_0(x)$ and $g(x)$ must have the same degree. The leading term of $bxf_0(x)$ is thus $bxc_r x^r = b\sigma(c_r)x^{r+1}$ and the leading term of $xg(x)$ is $xa_r x^r = \sigma(a_r)x^{r+1}$. The coefficients of these terms must be equal so we get $b\sigma(c_r) = \sigma(a_r)$ which implies that $b = \sigma(\frac{a_r}{c_r}) \in \sigma(F)$. This is a contradiction and so completes the proof. □

2.4 Wednesday 18 January 2012

2.4.1 Example of a ring which is left Noetherian but not right Noetherian

Example 23. The ring $R = \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} q_1 & q_2 \\ 0 & a \end{pmatrix} : q_1, q_2 \in \mathbb{Q}, a \in \mathbb{Z} \right\}$ is left Noetherian but not right Noetherian.

Proof. We'll show R is left Noetherian by showing any left ideal I is finitely generated. The first case here is if there is an element $\begin{pmatrix} q_1 & q_2 \\ 0 & q \end{pmatrix} \in R$ such that $a \neq 0$. Then for any $q \in \mathbb{Q}$ we have that $\begin{pmatrix} 0 & \frac{q}{a} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} q_1 & q_2 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & q \\ 0 & 0 \end{pmatrix} \in I$. Let $J = R\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Note that J is a finitely generated left ideal which lives in I and consists of all elements of R whose only nonzero element is in the upper right hand corner of the matrix. Define a ring homomorphism $\phi : R \to \mathbb{Q} \times \mathbb{Z}$ by $\begin{pmatrix} q_1 & q_2 \\ 0 & a \end{pmatrix} \longmapsto (q_1, a)$. By noticing that ϕ is surjective and that $\ker(\phi) = J$, we see that R/J is a ring, and that $R/J \cong \mathbb{Q} \times \mathbb{Z}$ as rings. Thus, R/J is left Noetherian, so the left ideal I/J is finitely generated and hence I is finitely generated because J is finitely generated.
The second case is if $I \subseteq \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & 0 \end{pmatrix} = W$. Note that W is a left ideal of R and so let $r = \begin{pmatrix} q_1 & q_2 \\ 0 & a \end{pmatrix} \in R$ and $\overline{w} = \begin{pmatrix} w_1 & w_2 \\ 0 & 0 \end{pmatrix} \in W$. then $r\overline{w} = \begin{pmatrix} q_1w_1 & q_1w_2 \\ 0 & 0 \end{pmatrix} \in W$. So we can consider W to be a $2-$dimensional $\mathbb{Q}$ vector space where scalar multiplication is given by $q\begin{pmatrix} w_1 & w_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} qw_1 & qw_2 \\ 0 & 0 \end{pmatrix}$. As $I \subseteq W$ is a $\mathbb{Q}-$subspace, then it has a basis of at most 2 elements, and so is finitely generated as a $\mathbb{Q}-$vector space. Also, a $\mathbb{Q}-$basis for I will be a finite generating set for I as a left ideal, so that I is finitely generated.
We'll now show R is not right Noetherian by producing an infinite ascending chain of right ideals. Let $I_n = \left\{ \begin{pmatrix} 0 & \frac{a}{2^n} \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Z} \right\}$ for any $n \geq 0$. Then $\begin{pmatrix} 0 & \frac{a}{2^n} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} q_1 & q_2 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & \frac{ab}{2^n} \\ 0 & 0 \end{pmatrix}$ so that since $ab \in \mathbb{Z}$ we get I_n is actually a right ideal of R. In fact, $I_n = \begin{pmatrix} 0 & \frac{1}{2^n} \\ 0 & 0 \end{pmatrix} R$. Since $\begin{pmatrix} 0 & \frac{1}{2^{n+1}} \\ 0 & 0 \end{pmatrix} \in I_{n+1} \setminus I_n$ then we get that this is an infinite properly ascending chain $I_0 \subsetneq I_1 \subsetneq \dots$ so that R is not right Noetherian. □

2.4.2 Simple & Semisimple rings & modules

Definition 24. Let M be a nonzero left $R-$module. M is said to be *simple* if (0) and M are the only submodules of M.

Note. This means that (0) is *not* simple. Also, there are simple rings that aren't simple modules, in fact $M_2(\mathbb{Q})$ is such an example.

Remark 25. A left $R-$module M is simple if and only if $M \cong R/I$ where I is a maximal left ideal of R.

Proof. ($\Rightarrow$) First, let M be simple and choose $x \in M \setminus \{0\}$. Then Rx is a left submodule of M so $M = Rx$ is cyclic. We define an $R-$linear map $\psi : R \to M$ given by $r \longmapsto rx$. Let $I = \ker \psi$ so that I is a left ideal of R. Note that ψ is surjective and so $R/I \cong M$. By the correspondence theorem, and since M is simple, we get that I is a maximal left ideal of R.
($\Leftarrow$) This direction is trivial. □

Definition 26. Let M be an $R-$module. M is called *semisimple* if every submodule of M is a direct summand of M. That is, if $N \subseteq M$ is a submodule of M, then there exists a submodule $N' \subseteq M$ such that $N \oplus N' = M$. Here $\oplus$ is the internal direct sum, meaning that $N + N' = M$ and $N \cap N' = (0)$.

Remark 27. The good news is that simple modules are semisimple. Unfortunately, there are simple rings which aren't semisimple.

Definition 28. A ring is called *left (resp. right) semisimple* if it is semisimple as a left (resp. right) module over itself.

Remark 29. If M is semisimple, then all submodules of M and all quotients of M are also semisimple.[4]

2.5 Friday 20 January 2012

2.5.1 Semisimple Modules

Example 30. Let D be a division ring. Then every $D-$module is semisimple.

Proof. Let V be a left $D-$module, and let W be a submodule of V. Let β be a basis for W. Then there exists a basis, β', of V which contains β. Let $\beta_1 = \beta' \setminus \beta$, and let W_1 be the span of β_1. Then $W_1 \oplus W = V$. □

Lemma 31. *Every nonzero semisimple module contains a simple module.*

[4] We sort of proved this in class.

Proof. Let $M \neq 0$ be a semisimple module, and choose $x \in M \setminus \{0\}$. Then $Rx \neq 0$ is semisimple as it is a submodule of M. Thus, we can assume $M = Rx$. Let $\Lambda = \{N : N \text{ is a submodule of } M, x \notin N\}$. By Zorn's Lemma, Λ has a maximal element, we'll call it N. As M is semisimple, $M = N \oplus N'$ for some N'. Also, note that $N' \neq 0$ as $x \notin N$. Then we claim that N' is simple. Let $A \neq 0$ be a submodule of N'. Since $A \nsubseteq N$, then $N + A \supsetneq N$. By maximality of N, $x \in N + A$ so that $N + A = M = Rx$. We wish to show that $A = N'$. Now, let $n' \in N' \subset M$. Then $n' = a + n$ for some $a \in A$ and $n \in N$. Rearranging this gives $n = n' - a \in N' \bigcap N = (0)$. Thus, $n' = a \in A$ so that $A = N'$. □

Theorem 32. *Let M be an $R-$module. TFAE:*

1. *M is semisimple,*
2. *M is a sum of simple submodules, that is, $M = \sum_{i \in I} N_i$ where each N_i is simple, and*
3. *M is a direct sum of simple submodules, that is, $M = \bigoplus_{i \in I} N_i$ where each N_i is simple.*

Proof. (1) ⇒ (3) If $M = (0)$, then we're done, so we may assume $M \neq (0)$. Let $T = \{N \mid N \text{ is a simple submodule of } M\}$. By the lemma $T \neq \emptyset$, so let

$$\Lambda = \left\{ J \subseteq T \mid \sum_{E \in J} E = \bigoplus_{E \in J} E \right\}.$$

Note that $\emptyset \in \Lambda$ so that $\lambda \neq \emptyset$. Let $\mathcal{C}$ be a totally ordered subset of Λ. We claim $A = \bigcup_{J \in \mathcal{C}} J \in \Lambda$. Suppose not. Then $\sum_{E \in A} \neq \bigoplus_{E \in A} E$ so that there exist $E_1, \ldots, E_n \in A$ such that $E_1 + \ldots + E_n \neq E_1 \oplus \ldots \oplus E_n$. But there is some $J \in \mathcal{C}$ such that $\{E_1, \ldots, E_n\} \subseteq J$. That forms a contradiction and so we have that $A \in \Lambda$. Thus, by Zorn's Lemma, there is some $J \in \Lambda$ which is maximal. Let $B = \sum_{E \in J} E = \bigoplus_{E \in J} E$. We claim that $B = M$. If not, then as M is semisimple, there is some $C \neq 0$ submodule of M such that $M = B \oplus C$. As C is semisimple, then by lemma 31 it contains some E' which is simple. Let $J' = J \cup \{E'\}$. Then $J' \in \Lambda$, which contradicts the maximality of J, and so $B = M$.
(3) ⇒ (2) Trivial.
(2) ⇒ (1) Let A be a submodule of M, let $T = \{N \mid N \text{ is a simple submodule of } M\}$, and let

$$\Lambda = \left\{ J \subseteq T \mid \sum_{E \in J} E = \bigoplus_{E \in J} E; A \bigcap \left(\sum_{E \in J} E \right) = (0) \right\}.$$

Again, $\emptyset \in \Lambda$, so that $\Lambda \neq \emptyset$. Also, we have that Zorn's Lemma applies, so let $J \in \Lambda$ be maximal, and set $A' = \sum_{E \in J} E = \bigoplus_{E \in J} E$. Let $B = A + A' = A \oplus A'$. Note that this is actually a direct sum as $J \in \Lambda$ means that $A \cap A' = (0)$. So we now claim that $B = M$. As M is a sum of simple submodules, it sufficies to show that every simple submodule of M is contained in B. Suppose not, that is, there is a simple submodule $E' \subseteq M$ with $E' \nsubseteq B$. Then $E' \cap B = (0)$ as E' is simple. Let $J' = J \cup \{E'\}$. Then $\left(\sum_{E \in J} E \right) + E' = \left(\bigoplus_{E \in J} E \right) \bigoplus E'$ as $E' \cap A' = (0)$ and $A \bigcap \left(\left(\sum_{E \in J} E \right) + E' \right) = (0)$.[5] Hence, $J' = J \cup \{E'\} \in \Lambda$ which contradicts the maximality of J. Thus, $B = A \oplus A' = M$ so that M is semisimple. □

2.6 Monday 23 January 2012

2.6.1 Composition Series & Length

Definition 33. Let M be an $R-$module. A *series (or filtration)* for M is a finite sequence of submodules

$$(0) = M_n \subseteq M_{n-1} \subseteq \ldots \subseteq M_0 = M.$$

The *factors* of the series is the set $\{M_i / M_{i+1}\}_{i=0}^{n-1}$. The *length* of the series is the number of proper inclusions. A *refinement* of a series is a series for M which contains the original series as a sub-series. A refinement is *proper* if the length of the refinement is larger than the length of the original series. Two series are *equivalent* if they have the same length and there is a bijection between the sets of factors such that corresponding factor modules are isomorphic.

Example 34. The sequence[6] $(0) \subsetneq (18) \subsetneq (3) \subsetneq \mathbb{Z}$ is a series with factors $\{(18), \mathbb{Z}/(6), \mathbb{Z}/(3)\}$. This series has the following series as a proper refinement: $(0) \subsetneq (72) \subsetneq (18) \subsetneq (9) \subsetneq (3) \subsetneq \mathbb{Z}$ with factors $\{(72), \mathbb{Z}/(4), \mathbb{Z}/(2), \mathbb{Z}/(3), \mathbb{Z}/(3)\}$. An equivalent series is $(0) \subsetneq (72) \subsetneq (24) \subsetneq (12) \subsetneq (4) \subsetneq \mathbb{Z}$ since this series has factors $\{(72), \mathbb{Z}/(3), \mathbb{Z}/(2), \mathbb{Z}/(3), \mathbb{Z}/(4)\}$.

[5] This isn't hard to show but isn't what I would call obvious either. The details are in my written notes.
[6] The notation (n) is used for $n\mathbb{Z} = \mathbb{Z}n$.

Lemma 35. *Let M be an $R-$module and $A \subseteq A'$, $B \subseteq B'$ submodules of M. Then*

$$\frac{A + (A' \cap B')}{A + (A' \cap B)} \cong \frac{B + (A' \cap B')}{B + (A \cap B')}.$$

Proof. The trick here[7] is to how that both modules are isomorphic to

$$\frac{A' \cap B'}{(A' \cap B) + (A \cap B')}.$$

Because of symmetry, it is sufficient to do this for only one of the modules in the statement. By defining

$$\psi : A + (A' \cap B') \to \frac{A' \cap B'}{(A' \cap B) + (A \cap B')}$$

via $a + x \longmapsto \overline{x}$ we can show that this is a surjective homomorphism with kernel equal to $A + (A' \cap B)$ so that by the first isomorphism theorem we're done. □

Theorem 36 (**Shreier Refinement Theorem**). *Any two series for a module M have equivalent refinements.*

Proof. Let

$$(0) = M_n \subseteq M_{n-1} \subseteq \ldots \subseteq M_0 = M \tag{2.2}$$

and

$$(0) = N_p \subseteq N_{p-1} \subseteq \ldots \subseteq N_0 = M \tag{2.3}$$

be two series for M. For $i \in \{0, \ldots, n-1\}$ and $j \in \{0, \ldots, p\}$ let $M_{i_j} = M_{i+1} + M_i \cap N_j$. Then for each i, j, we have $M_{i_j} \subseteq M_{i_{j-1}}$. Also, $M_{i_p} = M_{i+1}$ and $M_{i_0} = M_i$. This gives a refinement of (2.2) as

$$(0) \subseteq M_{n-1_p} \subseteq M_{n-1_{p-1}} \subseteq \ldots \subseteq M_{n-1_0} = M_{n-2_p} \subseteq \ldots \subseteq M_{n-2_0} \subseteq \ldots \subseteq M_{0_0} = M. \tag{2.4}$$

Similarly, for $i \in \{0, \ldots, n\}$, and $j \in \{0, \ldots, p-1\}$ let $N_{j_i} = N_{j+1} + M_i \cap N_j$. Again, we have for each i, j that $N_{j_i} \subseteq N_{j_{i-1}}$, that $N_{j_n} = N_{j+1}$, and $N_{j_0} = N_j$. So we again get a refinement, but this time of (2.3):

$$(0) = N_{p-1_n} \subseteq N_{p-1_{n-1}} \subseteq \ldots \subseteq N_{p-1_0} \subseteq N_{p-2_n} \subseteq \ldots \subseteq N_{p-2_0} \subseteq \ldots \subseteq N_{0_0} = N. \tag{2.5}$$

Now, the nonzero factors of (2.4) are $\{M_{i_j}/M_{i_{j+1}}\}$ and the nonzero factors of (2.5) are $\{N_{j_i}/N_{j_{i+1}}\}$. Then by the lemma, we get that

$$\frac{M_{i_j}}{M_{i_{j+1}}} = \frac{M_{i+1} + M_i \cap N_j}{M_{i+1} + M_i \cap N_{j+1}} \cong \frac{N_{j+1} + M_i \cap N_j}{N_{j+1} + M_{i+1} \cap N_j} = \frac{N_{j_i}}{N_{j_{i+1}}}$$

showing that the two refinements are equivalent. □

Definition 37. A *composition series* is a series with no proper refinements. In particular, in a composition series, all of the nonzero factor modules are simple.

Corollary 38 (**Jordan-Holder Theorem**). *If M has a composition series, then any two composition series for M are equivalent. In particular, they have the same length.*

Definition 39. If an $R-$module M has a composition series, then the *length of* M, which is denoted $\lambda_R(M)$ is the length of any composition series for M. If M has no composition series, then we define $\lambda_R(M) = \infty$.

Remark 40. 1. If M is a module of finite length, then any series can be refined to a composition series.
2. $\lambda_R(M) = 0$ implies that $M = 0$.
3. $\lambda_R(M) = 1$ implies that M is a simple module.

Proposition 41. *If $\lambda_R(M) < \infty$ and N is a submodule of M, then $\lambda_R(N) \leq \lambda_R(M)$ with equality holding if and only if $N = M$.*

Proof. Consider the series $0 \subseteq N \subseteq M$. As M has finite length, we can refine this to a composition series $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n \subseteq M$. Since this is a refinement, then for some $t \in \{0, \ldots, n\}$ we have $M_t = N$. Thus, $\lambda_R(N) = t \leq n = \lambda_R(M)$ and we clearly get that $n = t$ if and only if $N = M$. □

[7] I'm not going to go through all the details of this proof here.

2.7 Wednesday 25 January 2012

2.7.1 More on Length

Proposition 42. *Let M be a left $R-$module. Then M has finite length if and only if M is both Noetherian and Artinian.*

Proof. ($\Leftarrow$) Any ascending or descending chain of submodules of M can be refined to a composition series. Thus, any such chain has at most $\lambda_R(M)$ strict containments, so that any ascending or descending chain stabilizes.

($\Rightarrow$) If $M = 0$, then M clearly has length 0 so we may assume $M \neq 0$. Let $\Lambda = \{N \mid N \subseteq M; N \neq 0\}$. As M is Artinian, and $M \in \Lambda$, then there exists some $M_1 \in \Lambda$ which is minimal, and hence simple. If $M = M_1$, then $\lambda_R(M) = 1$. If not, then choose M_2 which is minimal among all submodules of M which properly contain M_1. Again, M_2/M_1 is clearly simple. Proceeding in this way we get $0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots$ where M_i/M_{i-1} is simple for all i. As M is Noetherian, we eventually have $M = M_n$ for some n so that we have a composition series, and hence finite length. □

Notation. If we are thinking of R as a left $R-$module we write ${}_RR$ and if we are thinking of R as a right $R-$module then we write R_R.

Corollary 43. *Suppose $\lambda_R({}_RR) < \infty$. Then any finitely generated left $R-$module, M, has finite length.*

Proof. Since $\lambda_R({}_RR) < \infty$ then R is left Noetherian and left Artinian. Thus, any finitely generated left $R-$module, M is Artinian and Noetherian, so that $\lambda_R(M) < \infty$. □

Proposition 44. *Let $0 \to L \to M \to N \to 0$ be a short exact sequence of $R-$modules. Then $\lambda_R(M) = \lambda_R(L) + \lambda_R(N)$.*

Proof. Since M is Noetherian (resp. Artinian) if and only if L and N are, then $\lambda_R(M) < \infty$ if and only if both $\lambda_R(L)$ and $\lambda_R(N)$ are finite. So we may assume $\lambda_R(M) < \infty$, so that L and N also both have finite length, and set $\ell = \lambda_R(L)$, and $n = \lambda_R(N)$. Without loss of generality, we may assume $L \subseteq M$ and $N = M/L$. We have composition series

$$0 = L_\ell \subsetneq L_{\ell-1} \subsetneq \ldots \subsetneq L_0 = L \tag{2.6}$$

and

$$0 = M_n/L \subsetneq M_{n-1}/L \subsetneq \ldots \subsetneq M_0/L = N. \tag{2.7}$$

This gives that

$$L = M_n \subsetneq M_{n-1} \subsetneq \ldots \subsetneq M_0 = M \tag{2.8}$$

with $M_i/M_{i+1} \cong \frac{M_i/L}{M_{i+1}/L}$ which is simple because (2.7) is a composition series. Combining (2.6) with (2.8) gives a composition series for M of length $\ell + n$:

$$0 = L_\ell \subsetneq L_{\ell-1} \subsetneq \ldots \subsetneq L_0 = L = M_n \subsetneq M_{n-1} \subsetneq \ldots \subsetneq M_0 = M.$$

□

Corollary 45. *By applying the proposition to the short exact sequence $0 \to A_1 \to A_1 \oplus A_2 \to A_2 \to 0$ we get $\lambda_R(A_1 \oplus A_2) = \lambda_R(A_1) + \lambda_R(A_2)$.*

Corollary 46. *By induction we then have $\lambda_R(\bigoplus_{i=1}^n A_i) = \sum_{i=1}^n \lambda_R(A_i)$.*

Example 47. Let D be a division ring, and M a finitely generated $D-$module. Since M has a finite basis, $M \cong \bigoplus_{i=1}^n D$ where $n = \dim_D(M)$. Thus, $\lambda_D(M) = \lambda_D(\bigoplus_{i=1}^n D) = \sum_{i=1}^n \lambda_D(D) = n = \dim_D(M)$.

Example 48. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/(12)$. Then the following series: $0 \subset (6)/(12) \subset (3)/(12) \subset \mathbb{Z}/(12) = M$ is a composition series for M so that $\lambda_R(M) = 3$.

Note. Since $\mathbb{Z}$ is Noetherian but not Artinian, we have that $\lambda_{\mathbb{Z}}(\mathbb{Z}) = \infty$.

Example 49. Let k be a field, $R = k[x]$, and $M = k[x]/(x^2) = k \cdot 1 \oplus k \cdot \overline{x}$. Consider the map $\varphi : R \to (x)/(x^2)$ given by $1 \longmapsto x + (x^2)$. This map is a surjection and $\ker(\varphi) = (x)$ so that $(x)/(x^2) \cong R/(x)$ and $R/(x) \cong k$ is simple. Also, $\frac{R/(x)}{(x)/(x^2)} \cong R/(x)$ by the isomorphism theorems. Thus, $0 \subsetneq (x)/(x^2) \subsetneq R/(x^2) = M$ is a composition series so that $\lambda_R(M) = 2 = \dim_k(M)$.

Example 50. Let $R = \mathbb{R}[x]$ and $M = \mathbb{R}[x]/(x^2+1) = \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot \overline{x}$. As (x^2+1) is a maximal ideal, then M is simple and $\lambda_R(M) = 1$. So here we have $\lambda_R(M) = 1 \lneq 2 = \dim_{\mathbb{R}}(M)$.

Example 51. Let $R = \mathbb{C}[x]$ and $M = \mathbb{C}[x]/(x^2+1) = \mathbb{C} \cdot 1 \oplus \mathbb{C} \cdot \overline{x}$. Then $0 \subsetneq (x-i)/(x^2+1) \subsetneq \mathbb{C}[x]/(x^2+1) = M$ is a composition series, so $\lambda_R(M) = 2 = \dim_{\mathbb{C}}(M)$.

Example 52. Let D be a division ring, $R = M_n(D)$ and $V = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \mid a_i \in D \right\}$. Then V is a left $R-$module. In fact, V is a simple $R-$module. It is enough here to show that if $\overline{v} \in V \setminus \{0\}$ then $R\overline{v} = V$, and this isn't hard to show as D is a division ring. So now, fix $i \in \{1, \ldots, n\}$ and let $I_i = \{[a_{k\ell}]_{n\times n} \mid a_{ki} = 0, a_{k\ell} \in R\}$. This is the set of matrices where the i^{th} column is nonzero, but all other columns are zero. Thus, for all i we have I_i is a left ideal of R and $I_i \cong V$ as left modules. It is clear that $R = \bigoplus_{i=1}^{n} I_i \cong V^n$, so that $\lambda_R(R) = \lambda_R(V^n) = n\lambda_R(V) = n$. However, note that $\dim_D(R) = n^2$.

2.8 Friday 27 January 2012

2.8.1 Semisimple Rings - Headed towards proving Artin-Wedderburn

Recall. A ring R is called left semisimple if ${}_RR$ is semisimple.

Example 53. 1. Any division ring D is left semisimple as ${}_DD$ is simple.
2. If D is a division ring then $R = M_n(D)$ is left semisimple. This can be seen by letting V be the set of $n\times 1$ (i.e. column) matrices over D. Then V is a simple left $R-$module and ${}_RR \cong V^n$ which proves that R is left semisimple. Symmetrically, R_R is isomorphic to W^n where W is the set of $1 \times n$ (i.e. row) matrices over D so that R_R is also semisimple.

Corollary 54. *Let $D_1, \ldots, D_k$ be division rings and $n_1, \ldots, n_k$ be positive integers. Then $M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$ is left (and right) semisimple.*

Comment. The following theorem is going to be our goal to prove for the next several class periods.

Theorem 55 (Artin-Wedderburn Theorem). *Let R be a left semisimple ring. Then there exist unique division rings $D_1, \ldots, D_k$ and integers $n_1, \ldots n_k$ such that $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$.*

Note. Note that by the previous Corollary, the Artin-Wedderburn Theorem implies that if R is left semisimple then R is right semisimple.

Proposition 56. *Let R be left semisimple. Then,*

1. *${}_RR = I_1 \oplus \ldots \oplus I_n$ where each I_j is a simple left ideal of R.*
2. *$\lambda_R({}_RR) < \infty$ (which then implies that R is left Noetherian and left Artinian)*
3. *Every simple left $R-$module is isomorphic to I_j for some j, where the I_j's are as in the first statement of the theorem.*

Proof. 1. Since we know that ${}_RR$ is semisimple, we have that ${}_RR = \bigoplus_{j\in\Lambda} I_j$ where each I_j is a simple left ideal of R. As $1 \in R$ we can write $1 = x_{j_1} + x_{j_2} + \ldots + x_{j_\ell}$ where each $x_{j_i} \in I_{j_i}$. Now, given any $r \in R$ we have that $r = r \cdot 1 = rx_{j_1} + \ldots + rx_{j_\ell}$ and each $rx_{j_i} \in I_{j_i}$ as each I_{j_i} is a left ideal of R. Thus, ${}_RR \subseteq \bigoplus_{i=1}^{\ell} I_{j_i}$ so that ${}_RR = I_{j_1} \oplus \ldots \oplus I_{j_\ell}$ and we can reindex these so we have ${}_RR = I_1 \oplus \ldots \oplus I_n$.
2. For each i we have that $\lambda_R(I_i) = 1$ since each I_i is simple. Thus by the additivity of length we get that $\lambda_R({}_RR) = \lambda_R(I_1 \oplus \ldots \oplus I_n) = \sum_{j=1}^{n} \lambda_R(I_j) = n$.
3. First, let J be a simple left ideal. Consider $0 \subseteq J \subseteq R$ as a series for ${}_RR$. This can be refined to a composition series since the length of R as a left module over itself is finite. So we get:

$$0 = J_n \subseteq J_{n-1} \subseteq \ldots \subseteq J_1 \subseteq J_0 = R$$

where $J_{n-1} = J$ since J is simple. We also have the following as a composition series for R:

$$0 \subseteq I_1 \subseteq I_1 \oplus I_2 \subseteq \ldots \subseteq I_1 \oplus \ldots \oplus I_n = R.$$

By the Jordan Holder Theorem (Corollary 38) we get that $J \cong I_i$ for some i since the factors of the second series here are the I_i's. Now, let M be a simple left $R-$module, and let $x \in M \setminus \{0\}$. As M is simple, we have that $M = Rx$. Now, define $\phi : R \to M$ via $r \longmapsto rx$. This is a surjective homomoprhism of left $R-$modules. Let $K = \ker\phi$. Thus, $R/K \cong M$ as left $R-$modules by the first isomorphism theorem. As ${}_RR$ is semisimple, we also have that $R = K \oplus I$ for some left ideal I. Thus, $M \cong R/K \cong \frac{K\oplus I}{K} \cong I$ and $I \cong I_i$ for some i by the previous argument. Thus, every simple left $R-$module is isomorphic to one of the I_i's.

□

Lemma 57. *Let R be a ring, I a simple left ideal, and M a simple left module. Then either $I \cong M$ or $IM = 0$.*

Proof. Suppose $IM \neq 0$. Then let $x \in M$ so that $Ix \neq 0$. Note that Ix is a left submodule of M, so as M is simple, we must have that $Ix = M$. Define, $\phi : I \to M$ by $a \longmapsto ax$. Note that ϕ is a surjective homomorphism of left $R-$modules since $M = Ix$. Now, if $\ker\phi = I$, then $Ix = 0$, which is a contradiction, and since I is simple, we then must have that $\ker\phi = 0$ so that ϕ is an isomorphism. □

Lemma 58 (Schur's Lemma). *Let R be a ring and M a simple left $R-$module. Then*

$$\mathrm{End}_R(M) = \{f : M \to M \mid f \text{ is a left } R-\text{linear map}\}$$

is a division ring.

Proof. Let $f \in \mathrm{End}_R(M)$ be chosen so that $f \neq 0$. Then $\mathrm{image}(f) \neq 0$ so that we must have $\mathrm{image}(f) = M$ since M is a simple module. Similarly, we cannot have $\ker(f) = M$ since $f \neq 0$ so we must have that $\ker(f) = 0$. Thus, f is an isomorphism, and so has an inverse in $\mathrm{End}_R(M)$. □

2.9 Monday 30 January 2012

2.9.1 Continuing to work towards Artin-Wedderburn

Proposition 59. *Let R be a left semisimple ring. Let $\{I_1, \ldots, I_k\}$ be the set of distinct (up to isomorphism) simple left ideals of R.*[8] *For each $i \in \{1, \ldots, k\}$, let $R_i = \sum L$ where the sum is taken over all left ideals, L, of R, such that $L \cong I_i$. Then*

1. *R_i is a ring with identity for all i.*
2. *R_i is left semisimple for all i.*
3. *R_i has one distinct (up to isomorphism) simple left ideal for each i.*
4. *R_i is simple for all i.*
5. *$R \cong R_1 \times \ldots \times R_k$ as rings.*

Proof. Recall from Lemma 57 that if I, J are simple left ideals, then $I \ncong J$ implies that $IJ = 0$. Hence, $R_iR_j = 0$ for $i \neq j$ and each R_i is a left ideal of R. Since R is semisimple, then $R = I_1 + \ldots + I_k \subseteq R_1 + \ldots + R_k \subseteq R$ by proposition 56. Fix some $x \in R$ and write $x = x_1 + \ldots + x_k$ with $x_i \in R_i$ for each i. We also have $1 = e_1 + \ldots + e_k$ where $e_i \in R_i$. Thus, $x_i = x_i \cdot 1 = x_ie_1 + \ldots + x_ie_k = x_ie_i = (x_1 + \ldots + x_k)e_i = xe_i$ since $x_je_\ell = 0$ whenever $j \neq \ell$. This means that each x_i is uniquely determined so that $R = R_1 \oplus \ldots \oplus R_k$. Since each R_i is a left ideal, they're closed under addition and multiplication, but we also want to show that they have identities. In particular, for any $r \in R_i$, then $r = r \cdot 1 = r(e_1 + \ldots + e_k) = re_i$ and similarly $e_ir = (e_1 + \ldots + e_k)r = 1 \cdot r = r$ so that e_i is the identity element of R_i so that R_i is a ring with identity. We can easily[9] check that the map $\phi : R \to R_1 \times \ldots \times R_k$ defined by $x \longmapsto x(e_1, \ldots, e_k)$ is an isomorphism, which completes the proof of parts 1 and 5.

Clearly, if $J \subseteq R_i$ is a left ideal of R, then J is a left ideal of R_i. Conversely, if $J \subseteq R_i$ is a left ideal of R_i, then J is also a left ideal of R since $RJ \subseteq RR_i = (R_1 + \ldots + R_k)R_i = R_iR_i \subseteq R_i$. Thus, the left ideals of R_i are precisely the left ideals of R which are contained in R_i. Now, since R_i is a left ideal of R, then by definition of R_i we get that R_i is left semisimple as an $R-$module, so it is a direct sum of simple left $R-$submodules. Thus, R_i is left semisimple as a ring, which completes the proof of 2.

Next, let $J \subseteq R_i$ be a simple left ideal. Then, using the same fact about the left ideals of R_i, we get that $J \cong I_j$ for some j. Hence, $J \cong I_i$, which gives 3.

Finally, let J be a nonzero (2-sided) ideal of R_i. In order to show R_i is simple, it is enough to show that $J \supseteq K$ for every left ideal K of R such that $K \cong I_i$. This is because R_i is defined to be the sum of all such ideals, so if J contains all of them, then $J = R_i$. So let K be any left ideal of R such that $K \cong I_i$. Since $J \neq 0$, and J is left semisimple, then it must contain a simple left ideal, say L. Clearly, we must have that $L \cong I_i$ and since $K \cong I_i$, then we know that $L \cong K$. Since R_i is semisimple, $R_i = L \oplus L'$ where L' is a left ideal of R_i. This gives that $e_i = \ell_1 + \ell_2$ where $\ell_1 \in L$ and $\ell_2 \in L'$. For any $\ell \in L$ we have $\ell = \ell e_i = \ell\ell_1 + \ell\ell_2$ so that $\ell\ell_2 = \ell - \ell\ell_1 \in L \cap L'$ so that $\ell\ell_2 = 0$ and hence $\ell = \ell\ell_1$ and $L = L\ell_1$. Now, let $\psi : L \to K$ be a left $R-$module isomorphism. Then $K = \psi(L) = \psi(L\ell_1) = L\psi(\ell_1) \subseteq J\psi(\ell_1) \subseteq J$ since J is an ideal. □

Corollary 60. *Let R be a left semisimple ring. The following are equivalent:*

1. *R is simple.*
2. *R has a unique (up to isomorphism) simple left module.*

Corollary 61. *If R is a simple ring which is also left semisimple, then R is left Artinian.*

2.10 Wednesday 1 February 2012

2.10.1 Rieffel's Theorem & Most of proof of Artin-Wedderburn

Definition 62. Let R be a ring. We define here the *opposite ring of R*, which is denoted R^{op}. As a set R^{op} is in bijective correspondence with R and we write a^o as the element in R^{op} which corresponds to $a \in R$. The operations on R^{op} are as follows:

$$a^o + b^o = (a + b)^o \quad \text{and} \quad a^o \cdot b^o = (ba)^o.$$

Remark 63. For any ring R, we get $\mathrm{End}_R(R) \cong R^{op}$. This isomorphism can be shown using the map $f : \mathrm{End}_R(R) \to R^{op}$ given by $\phi \longmapsto (\phi(1))^o$.

[8] We know this set is finite by Proposition 56.

[9] I didn't carefully write the details, but I thought through them, and they're not hard.

Example 64. Let M be a left $R-$module. Then $M^n = M \oplus \ldots \oplus M$ where there are n copies of M in the direct sum. Also, if we define M_i to be $M_i = \{(0, \ldots, m, \ldots, 0) \mid m \in M\} \subseteq M^n$ where the m is in the i^{th} spot for a given i, then we have the usual inclusion and projection maps: $\rho_i : M_i \hookrightarrow M^n$ and $\pi_i : M^n \twoheadrightarrow M_i$. For $\psi \in \mathrm{End}_R(M^n)$ let $\psi_{ij} : M \to M$ be the composition of the following maps:

$$M \cong M_i \xhookrightarrow{\rho_i} M^n \xrightarrow{\psi} M^n \xrightarrow{\pi_j} M_j \cong M$$
$$\psi_{ij}$$

so that $\psi_{ij} \in \mathrm{End}_R(M)$ for all i, j. It is a fact that the map $\mathrm{End}_R(M^n) \to M_n(\mathrm{End}_R(M))$ given by $\psi \longmapsto [\psi_{ij}]_{n\times n} = [\psi]$ is a ring homomorphism.[10] A special case is when $M =_R R$; then $\mathrm{End}_R(R^n) \cong M_n(\mathrm{End}_R(R)) \cong M_n(R^{op})$.

Notation. Let M be a left $R-$module. We define

$$R' = R'(M) := \mathrm{End}_R(M)$$

and note here that M is a left $R'-$module where we set $\phi \cdot x = \phi(x)$ for any $\phi \in R'$ and $x \in M$. We also define

$$R'' = R''(M) := \mathrm{End}_{R'}(M).$$

For a given $a \in R$, we have the map $\ell_a : M \to M$ by $x \longmapsto ax$ and we note that for any $a \in R$, $\phi \in R'$ and $x \in M$ then $\ell_a(\phi \cdot x) = \ell_a(\phi(x)) = a\phi(x) = \phi(ax) = \phi \cdot ax = \phi \cdot \ell_a(x)$ since ϕ is an $R-$linear map. Hence, $\ell_a \in R''(M)$. Similarly if I is a left ideal of R, and $a \in I$ then $r_a : I \to I$ given by $x \longmapsto xa$ is an element of $R'(I)$ since $r_a(bx) = bxa = br_a(x)$ for any $b \in R$ and $x \in I$.

Remark 65. The map $\lambda : R \to R''(M)$ given by $a \longmapsto \ell_a$ is a ring homomorphism.

Proof. Given any $r, s \in R$ we have $\lambda(r + s) = \ell_{r+s}$ which is the map from M to M given by left multiplication by $r + s$ and this is equal to $\ell_r + \ell_s = \lambda(r) + \lambda(s)$ since M is a module. Also, $\lambda(rs) = \ell_{rs}$ is left multiplication by rs. We have for any $x \in M$ that $\ell_{rs}(x) = rsx = r(sx) = \ell_r(\ell_s(x)) = \ell_r\ell_s(x)$ so that $\lambda(rs) = \lambda(r)\lambda(s)$ and we do indeed have a ring homomorphism. □

Theorem 66 (Rieffel). *Let R be a simple ring, and I a nonzero left ideal of R. Then $\lambda : R \to R''(I)$ given by $a \longmapsto \ell_a$ is an isomorphism.*

Proof. Since R is a simple ring, we know that $\ker(\lambda) = 0$ or R. However, $\lambda(1) = \ell_1 \neq 0$ so we must have that $\ker(\lambda) = 0$ and λ is injective. Now, we claim that $\lambda(I)$ is a left ideal of $R'' = R''(I)$. To show this, let $f \in R'' = \mathrm{End}_{R'}(I)$ and let $\ell_a \in \lambda(I)$. We have $f\ell_a(x) = f(ax) = f(r_x(a)) = f(r_x \cdot a) = r_x f(a) = f(a)x = \ell_{f(a)}(x)$ since $r_x \in R'(I)$ and so we get that $f\ell_a = \ell_{f(a)} \in \lambda(I)$ and since it is clear that $\lambda(I)$ is an additive subgroup of $R''(I)$, we get that $\lambda(I)$ is a left ideal of $R''(I)$. Consider the (2-sided) ideal IR of R.[11] Since R is simple and $IR \neq 0$ we must have that $IR = R$. Thus, $\lambda(R) = \lambda(IR) = \lambda(I)\lambda(R)$. Finally, using the fact that $1_{R''} = \ell_1 \in \lambda(R)$ and that $\lambda(I)$ is a left ideal of R'' we get that

$$\begin{aligned} R'' &= R''\lambda(R) \\ &= R''\lambda(I)\lambda(R) \\ &\subseteq \lambda(I)\lambda(R) \\ &= \lambda(R) \end{aligned}$$

so that λ is surjective. □

Theorem 67. *Let R be a simple ring. The following are equivalent:*

1. *R is left semisimple,*
2. *R is left Artinian, and*
3. *$R \cong M_n(D)$ for some division ring D and $n \in \mathbb{N}$.*

Proof. ($3 \Rightarrow 1$) We've already shown this. See Example 52.
($1 \Rightarrow 2$) We've already shown this too. See Corollary 61.
($2 \Rightarrow 3$) Since R is left Artinian, it contains a simple left ideal I. (We can do this by choosing a minimal element of the set of nonzero left ideals). By Rieffel's Theorem (Theorem 66), we know that $R \cong R''(I) = \mathrm{End}_{R'}(I)$. By Schur's Lemma

[10] The additive part is easy enough, and I think the multiplicative part just comes from being careful about indices and matrix multiplication, but I haven't gotten it to work quite right.
[11] Recall that $IR = \{\sum_{k=1}^{n} i_k r_k \mid i_k \in I, r_k \in R, n \in \mathbb{N}\}$.

(Lemma 58) we know that $R' = \text{End}_R(I)$ is a division ring since I is simple, so we'll set $D = R'$. We now claim that I is finitely generated as an R' module and prove it by contradiction. If I is not finitely generated, then there is an infinite set $S = \{e_1, e_2, e_3, \ldots\} \subseteq I$ such that S is linearly independent over R'. For each n, let $J_n = \{f \in R'' \mid f(e_1) = \ldots = f(e_n) = 0\}$. Note that J_n is itself a left ideal of R'' for each n. Also, $J_n \supseteq J_{n+1}$ for all n. In fact, we have strict containment since there is an element $g \in R''$ such that $g(e_i) = 0$ for all $i \neq n+1$ and $g(e_{n+1}) = 1$ which is also an element of $J_n \backslash J_{n+1}$. Since $R'' \cong R$ this is a contradiction since we know R is left Artinian. Hence, for some $n \in \mathbb{N}$ we have $I \cong D^n$ as left $D-$modules. This means that $R \cong \text{End}_D(D^n) = M_n(D^{op})$. Note that D^{op} is also a division ring to complete the proof. □

2.11 Friday 3 February 2012

2.11.1 Artin-Wedderburn Modulo Uniqueness

Corollary 68. *Let R be a ring. The following are equivalent:*

1. *R is left semisimple*
2. *R is right semisimple*
3. *$R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$ where each D_i is a division ring and $n_i \in \mathbb{N}$ for each i.*

Proof. ($1 \Rightarrow 3$) We showed in Proposition 59 that $R \cong R_1 \times \ldots \times R_k$ where each R_i is simple and left semisimple. By Rieffel's Theorem (Theorem 66), we have that each $R_i \cong M_{n_i}(D_i)$ for some $n_i \in \mathbb{N}$ and division ring D_i.
($3 \Rightarrow 2$) Each $M_{n_i}(D_i)$ is right semisimple and a finite product of right semisimple rings is right semisimple. We proved this on the left on homework #2 but the proof on the right follows by mutatis mutandis.[12]
($2 \Rightarrow 1$) Since R is right semisimple, then R^{op} is left semisimple. Using the implication ($1 \Rightarrow 3$) we have that $R^{op} \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$ for $n_i \in \mathbb{N}$ and D_i a division ring for each i. Now,

$$R = (R^{op})^{op} \cong (M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k))^{op} \cong M_{n_1}(D_1^{op}) \times \ldots \times M_{n_k}(D_k^{op})$$

and since D_i^{op} is also a division ring for each i. Then by the same problem in homework #2 and since $M_n(D)$ is left semisimple for any $n \in \mathbb{N}$ and any division ring D, we get that R is left semisimple . □

Remark 69. Suppose that R is semisimple. Then $\lambda_R({}_RR) < \infty$ and $\lambda_R(R_R) < \infty$.

Exercise. If $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$ where each $n_i \in \mathbb{N}$ and each D_i is a division ring, then $\lambda_R({}_RR) = \lambda_R(R_R) = n_1 + \ldots + n_k$.

Question. If $\lambda_R({}_RR)$ and $\lambda_R(R_R)$ are both finite, are they necessarily equal?[13]

Remark 70. We will prove the uniqueness part of Artin-Wedderburn, but we need some more machinery first.

2.11.2 The map $\lambda : R \to R''(M)$

Remark 71. Given a map $f : E \to E$, then $f \in R''(E)$ if and only if f is both additive and $f \circ \phi = \phi \circ f$ for all $\phi \in R'(E)$. This is since $f(\phi(x)) = f(\phi \cdot x) = \phi \cdot f(x) = \phi(f(x))$ for all $f \in R''(E)$ and $\phi \in R'(E)$.

Remark 72. Let $f \in \text{End}_{R'}(E) = R''(E)$, and let $n \in \mathbb{N}$. Define $f^{(n)} : E^n \to E^n$ by $(x_1, \ldots, x_n) \longmapsto (f(x_1), \ldots, f(x_n))$. Then $f^{(n)} \in R''(E^n) = \text{End}_{R'(E^n)}(E^n)$.

Proof. It is clear that $f^{(n)}$ is additive, so we merely need to show that $f^{(n)}\psi = \psi f^{(n)}$ for any $\psi \in R'(E^n)$. We can write this using matrix notation as $\psi = [\psi_{ij}]_{n \times n}$ where $\psi_{ij} \in \text{End}_R(E) = R'(E)$ and $f^{(n)} = fI_n$. Thus, since $f \in R''(E)$ we have $f\psi_{ij} = \psi_{ij} f$ for all i, j and hence $f^{(n)}\psi = fI_n[\psi_{ij}] = [f\psi_{ij}] = [\psi_{ij} f] = [\psi_{ij}]fI_n = [\psi_{ij}]f^{(n)}$. □

Lemma 73. *Let E be a semisimple left $R-$module, $f \in R''(E)$ and $x \in E$. Then there exists some $a \in R$ such that $f(x) = \ell_a(x) = ax$.*[14]

Proof. As E is semisimple, then we have $E = Rx \otimes N$ for some submodule N. Let $\pi : E \to E$ be defined by $\pi(rx + n) = rx$. Then π is $R-$linear, meaning that $\pi \in R'(E)$ so that $f(x) = f(\pi(x)) = \pi(f(x)) \in Rx$. □

Theorem 74 (Jacobsen Density Theorem). *Let R be a ring, and E a semisimple $R-$module. Let $f \in R''(E)$ and $x_1, \ldots, x_n \in E$. Then there exists some $a \in R$ such that $f(x_i) = \ell_a(x_i)$ for all i.*

Proof. As we noted before, $f^{(n)} \in R''(E)$ and E^n is semisimple. So let $x = (x_1, \ldots, x_n) \in E^n$. By Lemma 73, there is some $a \in R$ such that $f^{(n)}(x) = \ell_a(x)$. Rewriting this gives $(f(x_1), \ldots, f(x_n)) = f^{(n)}(x) = \ell_a(x) = ax = (ax_1, \ldots, ax_n)$. Thus, $f(x_i) = \ell_a(x_i)$ for each $i = 1, \ldots, n$. □

[12] The statement in the homework was: Let $R_1, \ldots, R_n$ be rings and $R = R_1 \times \cdots \times R_n$. Prove that R is left semisimple if and only if R_i is left semisimple for $i = 1, \ldots, n$.

[13] Tom Marley seemed unsure if this was true or not, but didn't claim it was an open question.

[14] Note here that a will depend on x.

Corollary 75. *If R is a ring, E is a semisimple $R-$module, and E is finitely generated over $R'(E)$, then $\lambda : R \to R''(E)$ given by $a \longmapsto \ell_a$ is surjective.*

Proof. Let $E = R'x_1 + \ldots + R'x_n$ and let $f \in R''(E)$. Then the Jacobsen Density Theorem (Theorem 74) says that there is some $a \in R$ such that $f(x_i) = \ell_a(x_i)$ for each i. Then since f and ℓ_a are $R'-$linear, we get that $f = \ell_a = \lambda(a)$ so that λ is surjective. □

Corollary 76. *If R is a simisimple ring, and E is a free left $R-$module, then $\lambda : R \to R''(E)$ is an isomorphism.*

Proof. As R is semisimple, so is E. Let $e \in E$ be part of an $R-$basis for E. Then $E = R'e$ since we can send a basis element anywhere. Hence E is finitely generated over R' and so by Corollary 75, we have that λ is surjective. If $a \in \ker\lambda$ then $\ell_a(E) = 0$ so that $ae = 0$. This means that $a = 0$ as e is in a basis for E. Hence, λ is injective and thus an isomorphism. □

Example 77. Let A be the Weyl algebra (the long example from homework #1). Recall that A is simple but not left or right Artinian. Let E be any simple left $A-$module and consider the map $\lambda : A \to A''(E)$. As A is simple, and $\ker\lambda$ is an ideal, then λ is injective. Since E is simple, we get that $E = Ax$ for any $x \in E \setminus \{0\}$ so that E is a finitely generated $A-$module. **If** we were to have that E was finitely generated as an $A'-$module, then the first corollary implies that λ is surjective. This then gives that $A \cong A''(E) = \mathrm{End}_{A'}(E)$. Note that by Schur's Lemma (Lemma 58), A' is a division ring since E is simple. Then $E = (A')^n$ so that $A \cong \mathrm{End}_{A'}((A')^n) \cong M_n((A')^{op})$ which means that A is semisimple. This is a contradiction, and so we conclude that E is not finitely generated as an $A'-$module.

Remark 78. The arguments above give a different way to prove all but the uniqueness of the Artin-Wedderburn Theorem.

2.12 Monday 6 February 2012

2.12.1 End of proof of Artin-Wedderburn

Corollary 79. *Let D be a division ring, and V be a $D-$module. Then $\lambda : D \to \mathrm{End}_{D'}(V)$ is an isomorphism, where $D' = \mathrm{End}_D(V)$.*[15]

Proof. V is free and semisimple because D is a division ring, and so the hypotheses of Corollary 76 are satisfied and hence λ is an isomorphism. □

Corollary 80. *Let D_1 and D_2 be division rings. Suppose that $M_{n_1}(D_1) \cong M_{n_2}(D_2)$. Then $n_1 = n_1$ and $D_1 \cong D_2$.*

Proof. We'll first show $D_1 \cong D_2$. Recall from Example 64 that $M_{n_i}(D_i) \cong \mathrm{End}_{D_i^{op}}((D_i^{op})^n)$ for $i = 1, 2$. So we have that $\mathrm{End}_{D_1^{op}}((D_1^{op})^n) \cong \mathrm{End}_{D_2^{op}}((D_2^{op})^n)$. If we can show that for any division rings D_1 and D_2 and natural numbers n_1 and n_2 we have that $\mathrm{End}_{D_1}(D_1^{n_1}) \cong \mathrm{End}_{D_2}(D_2^{n_2})$ implies that $D_1 \cong D_2$ then we'll know that $D_1^{op} \cong D_2^{op}$ and hence $D_1 \cong D_2$. So let $R = \mathrm{End}_{D_1}(D_1^{n_1})$. Note that R is simple by Schur's Lemma (Lemma 58), and semisimple by part 2 of Example 53. Also, $D_1^{n_1}$ and $D_2^{n_2}$ are simple left $R-$modules since any single element of either can be extended to give a basis, and basis elements can be sent anywhere by endomorphisms. Now, since R is Artinian and simple, then it has precisely one simple module, up to isomorphism, and so $D_1^{n_1} \cong D_2^{n_2}$ as $R-$modules. Hence, $D_1 \cong \mathrm{End}_R(D_1^{n_1}) \cong \mathrm{End}_R(D_2^{n_2}) \cong D_2$. Now, we have that $M_{n_1}(D_1) \cong M_{n_2}(D_1)$ but that holds only if $n_1 = n_2$, which completes the proof. □

Lemma 81. *Suppose $\phi : A_1 \times \ldots \times A_k \to B_1 \times \ldots \times B_\ell$ is an isomorphism where A_i and B_j are simple rings for each i and j. Then $k = \ell$ and after reordering $A_i \cong B_i$ for each i.*

Proof. Let $I_1 = A_1 \times (0) \times \ldots \times (0)$. Then $\phi(I_1)$ is an ideal of $B_1 \times \ldots \times B_\ell$. So after rearranging, we get $\phi(I_1) \cong B_1 \times \ldots \times B_t \times (0) \times \ldots \times (0)$. As rings, we have $A_1 \cong \phi(I_1)$, so $\phi(I_1)$ has exactly two ideals, and hence $t = 1$. Now, by modding out by I_1 and $\phi(I_1)$ respectively, we have that $A_2 \times \ldots \times A_k \cong B_2 \times \ldots \times B_\ell$ and using induction on this argument completes the proof. □

Corollary 82 (Uniqueness of Artin Wedderburn Theorem). *If $M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k) \cong M_{m_1}(D_1') \times \ldots \times M_{m_\ell}(D_\ell')$ where D_i and D_i' are division rings, and n_i and m_i are positive integers. Then $k = \ell$, and (after rearranging) we have $D_i \cong D_i'$, and $n_i = m_i$ for each i.*

2.12.2 More about $\lambda : R \to R''$

Definition 83. Let $\phi : R \to S$ be a ring homomorphism such that $\phi(R) \subseteq Z(S) = \{s \in S \mid sx = xs \text{ for all } x \in S\}$. then S is an *R-algebra*. We say S is a *finitely generated $R-$algebra* if S is finitely generated as a ring over $\phi(R)$.

Remark 84. We frequently assume (by modding out by $\ker\phi$), that $R \subseteq S$ and $S = R[u_1, \ldots, u_n]$ for some $u_i \in S$, but that the u_i's do not commute.

Remark 85. Let R be a ring, and E an $R-$module.

[15] Recall that this map λ is given by $\lambda(a) = \ell_a$ and ℓ_a is left multiplication by a.

1. If $r \in Z(R)$, then $\ell_r \in R'(E)$ since $\ell_r(ax) = r(ax) = a(rx) = a\ell_r(x)$. Thus, $Z(R) \cdot \ell_1 \subseteq R'(E)$.
2. If E is finitely generated as a $Z(R)-$module, then E is finitely generated as an $R'(E)-$module.

Proof. Let $E = Z(R)u_1 + \ldots + Z(R)u_n$ for some $u_1, \ldots, u_n \in E$. Then, we have

$$\begin{aligned} E &= Z(R)u_1 + \ldots + Z(R)u_n \\ &= Z(R)\ell_1 u_1 + \ldots + Z(R)\ell_1 u_n \\ &\subseteq R'u_1 + \ldots + R'u_n \\ &\subseteq E \end{aligned}$$

since E is also an $R' = R'(E)$ module. □

Proposition 86. *Suppose R is finitely generated as a $Z(R)-$module, and that E is a finitely generated, semisimple $R-$module. Then $\lambda : R \to R''(E)$ is surjective.*

Proof. We have $R = Z(R)u_1 + \ldots + Z(R)u_n$ and $E = Rw_1 + \ldots + Rw_m$. Then $E = \sum Z(R)u_i w_j$, so that E is finitely generated as a $Z(R)-$module. By the second remark in Remark 85, we have that E is finitely generated as an $R'(E)-$module. Corollary 75 then tells us that λ is surjective. □

Corollary 87. *Let R be a finite dimensional $k-$algebra, where k is a field. That is, $k \subseteq Z(R)$ and $\dim_k(R) < \infty$. Also, let E be a finitely generated, semisimple $R-$module. Then $\lambda : R \to R''(E)$ is surjective.*

Theorem 88 (Burnside). *Let k be an algebraically closed field, and V a finite dimensional $k-$vector space. Let R be a subring of $\mathrm{End}_k(V)$ with $k \subseteq R$.[16] If V is a simple $R-$module, then $k = \mathrm{End}_R(V)$ and $R = \mathrm{End}_k(V)$.*

Proof. As $k \subseteq Z(R)$, then $k \subseteq \mathrm{End}_R(V) \subseteq \mathrm{End}_k(V)$. Since $\dim_k \mathrm{End}_k(V) < \infty$, then $\dim_k \mathrm{End}_R(V) < \infty$. Since V is a simple $R-$module, then $\mathrm{End}_R(V)$ is a division ring. Let $\alpha \in \mathrm{End}_R(V)$, and consider the (commutative) ring $k[\alpha]$. As $k[\alpha] \subseteq \mathrm{End}_R(V)$, then $k[\alpha]$ is a domain because by Schur's Lemma (Lemma 58), we have that $\mathrm{End}_R(V)$ is a division ring since V is simple. Also, $k[\alpha]$ is finite dimensional over k since $\mathrm{End}_R(V)$ is a finite dimensional $k-$vector space. Hence, $k[\alpha]$ is a field, and algebraic over k, so we get $\alpha \in k$ and hence $k = \mathrm{End}_R(V)$. Next, since V is simple, then V is also semisimple. Because, V is a finitely generated $R'-$vector space (since $R' = k$), we have by Corollary 75, that $\lambda : R \to R''(V) = \mathrm{End}_{R'}(V) = \mathrm{End}_k(V)$ is surjective. Also, λ is the inclusion map, so we must have $R = \mathrm{End}_k(V)$.[17] □

2.13 Wednesday 8 February 2012

2.13.1 Finishing off information about $\lambda : R \to R''$

Proposition 89. *Suppose that E is an $R-$module and $\lambda : R \to R''(E)$ is an isomorphism. Then $Z(R') = Z(R)\ell_1$.*

Proof. We've already seen that $Z(R)\ell_1 = \{\ell_r \mid r \in Z(R)\} \subseteq R'(E)$ in the first part of Remark 85. Let $f \in R'$ and $r \in Z(R)$. Then for any $e \in E$, we have $(f \circ \ell_r)(e) = f(re) = rf(e) = (\ell_r \circ f)(e)$, so that $f\ell_r = \ell_r f$ and $\ell_r \in Z(R')$ and hence $Z(R)\ell_1 \subseteq Z(R')$. Now, if $g \in Z(R')$, then for all $f \in R'$, we have $f(g(e)) = g(f(e))$. Equivalently, $g(f \cdot e) = f \cdot g(e)$ so that g is $R'-$linear and $g \in R'' = \lambda(R) = \{\ell_r \mid r \in R\}$. Hence, $g = \ell_r$ for some $r \in R$. We must now show that $r \in Z(R)$. We know that for all $s \in R$, that $rs \cdot e = g(s \cdot e) = s \cdot g(e) = sr \cdot e$ for all $e \in E$. Thus, $(rs - sr)E = 0$ so that $\ell_{rs-sr} = 0$. As λ is an isomorphism, then $rs - sr = 0$ so that $r \in Z(R)$. □

Corollary 90. *If D is a division ring, and V is a $D-$vector space, then by setting $R = D$ and $V = E$, we then have $Z(M_n(D)) = Z(D)I_n = \{rI_n \mid r \in Z(D)\}$. Also, $M_n(D) \cong \mathrm{End}_{D^{op}}(V)$ where $V = (D^{op})^n$.*

2.13.2 The Jacobsen Radical

Remark 91. Let R be a ring. Every proper left ideal of R is contained in a maximal left ideal of R. (The proof of this is by Zorn's Lemma).

Definition 92. Let R be a ring. The *Jacobsen radical of R*, denoted $J(R)$, is $J(R) = \bigcap m$ where the intersection is taken over all maximal left ideals of R.

Lemma 93. *Let R be a ring, and $y \in R$. The following are equivalent:*

1. *$y \in J(R)$,*
2. *$1 - xy$ is left invertible for every $x \in R$, and*
3. *$yM = 0$ for every simple left $R-$module, M.*

[16] Here, we are identifying an element, a, of k with the endomorphism given by multiplication by a.
[17] Some of this is from Wednesday's class, but it is nicer not to break up the proof in the notes.

Proof. $(1 \Rightarrow 2)$ Let $x \in R$. Suppose that $1 - xy$ is not left invertible. Then $R(1 - xy)$ is a proper left ideal. Let m be a maximal left ideal containing $R(1 - xy)$. Then $1 - xy \in m$. But $y \in J(R)$ implies that $y \in m$ so that $xy \in m$ and hence $1 \in m$ which is a contradiction and so we must have that $1 - xy$ is left inevertible.
$(2 \Rightarrow 3)$ Let M be a simple left $R-$module, and suppose $yM \neq 0$. Then there is some $u \in M$ such that $yu \neq 0$. Since M is simple, then $Ryu = M$, and there is some $r \in R$ such that $ryu = u$. Thus, $(1 - ry)u = 0$ but as $1 - ry$ is left invertible by hypothesis, then we must have that $u = 0$. This is a contradiction as we couldn't have had $u = 0$ and so $yM = 0$.
$(3 \Rightarrow 1)$ Let m be a maximal left ideal. Then R/m is simple and by assumption we have $yR/m = 0$ so we must have $y \in m$ and so $y \in J(R)$ as m was an arbitrary choice of maximal left ideal of R. □

Definition 94. Let M be a left $R-$module. The *annihilator of* M is $\mathrm{Ann}_R(M) = \{r \in R \mid rM = 0\}$.

Remark 95. 1. $\mathrm{Ann}_R(M)$ is always a (2-sided) ideal. This is because if $r \in \mathrm{Ann}_R(M)$ and $s \in R$, then $(rs)M = r(sM) \subseteq rM = 0$, and $(sr)M = s(rM) = s \cdot 0 = 0$.
2. Warning!!! If $x \in M$, then $\mathrm{Ann}_R(x) = \{r \in R \mid rx = 0\}$ is a left ideal, but it is not necessarily a 2-sided ideal.

Corollary 96. *Let R be a ring. Then $J(R) = \bigcap \mathrm{Ann}_R(M)$ where the the intersection is taken over all simple left $R-$modules, M. Hence, $J(R)$ is a $2-$sided ideal.*

Proof. This is from $1 \Leftrightarrow 3$ in the lemma. □

Proposition 97. *Let R be a ring, and $y \in R$. The following are equivalent:*

1. $y \in J(R)$, and
2. $1 - xyz$ is a unit for all $x, z \in R$.

Proof. $(1 \Rightarrow 2)$ Let $y \in J(R)$, and $x, z \in R$. Then $yz \in J(R)$ so $1 - xyz$ is left invertible by Lemma 93. Let u be a left inverse of $1 - xyz$, so that u is right invertible. We have $1 = u(1 - xyz) = u - uxyz$ so that $u = 1 - (-u)(xyz)$. Since $xyz \in J(R)$, then u is left invertible. Thus, u is a unit and $u^{-1} = 1 - xyz$ is also a unit.
$(2 \Rightarrow 1)$ Let $z = 1$. Then $1 - xy$ is a unit and hence left invertible for all $x \in R$, so that $y \in J(R)$ by Lemma 93 □

Corollary 98. *$J(R) = \bigcap m$ where this time the intersection is over all maximal right ideals, m, of R.*

2.14 Friday 10 February 2012

2.14.1 Semiprimitive Rings

Definition 99. A ring R is called *semiprimitive* if $J(R) = 0$. Apparently some people call this Jacobsen-semisimple, or simply J-semisimple.[18]

Example 100. 1. Any semisimple ring is semiprimitive.

Proof. Let R be a semisimple ring. Then we know $R = I_1 \oplus \ldots \oplus I_n$ where each I_i is a simple left ideal of R. This means we can write $1 = u_1 + \ldots + u_n$ where $u_i \in I_i$ for each i. For any $y \in J(R)$ we then have $yu_i = 0$ for all i since I_i is a simple left $R-$module. Thus, $y \cdot 1 = yu_1 + \ldots + yu_n = 0$ so that $y = 0$, and hence $J(R) = 0$. □

2. Any simple ring is semiprimitive because $J(R)$ cannot equal R.
3. $\mathbb{Z}$ is semiprimitive since the maximal ideals are $\{p\mathbb{Z} \mid p \text{ prime}\}$.
4. If F is a field, then $F[x]$ is semiprimitive because the maximal ideals are generated by prime elements, and there are infinitely many of them so that only the 0 polynomial can divide all of them.

Proposition 101. *Let R be a ring. The following are equivalent:*

1. R is semisimple, and
2. R is left Artinian and $J(R) = 0$.

Proof. $(1 \Rightarrow 2)$ We've already seen that semisimple rings are left Artinian from Theorem 67, and semiprimitive from the first part of Example 100.
$(2 \Rightarrow 1)$ To show this, we start by claiming that any simple left ideal, I, of R is a direct summand of R. Since $I \neq 0$ we know that $I \not\subset J(R) = 0$. Thus, there is a maximal left ideal m such that $I \not\subset m$. By the maximality of m, we get $I + m = R$, and $I \cap m = (0)$ since I is simple. Thus, $R = I \oplus m$ as desired. Now, since R is left Artinian, then any nonzero left ideal, L, contains a simple left ideal. This is easily seen by choosing a minimal element of the nonempty set $\Lambda = \{\text{nonzero left ideals contained in } L\}$. Let R_1 be a simple left ideal of R. By what we've already shown, we have that $R = I_1 \oplus A_1$ for some left ideal A_1. If $A_1 = (0)$, then we're done. So we assume $A_1 \neq (0)$. By the same reasoning, A_1 contains a simple left ideal, I_2. We have $R = I_2 \oplus A_2$ and now, $A_1 = (A_1 \cap R) = A_1 \cap (I_2 \oplus A_2) = I_2 \oplus (A_1 \cap A_2)$ so that $R = I_1 \oplus I_2 \oplus (A_1 \cap A_2)$. This gives a descending sequence of left ideals: $A_1 \supseteq A_1 \cap A_2 \supseteq \ldots$ and since R is Artinian, this sequence must stabilize, and so we must eventually have $A_1 \cap \ldots \cap A_n = 0$. Hence, $R = I_1 \oplus \ldots \oplus I_n$ and R is hence semisimple. □

[18] No pun intended.

2.14.2 Nilpotence

Definition 102. Let R be a ring, and I a left ideal. We say I is *nil* if every element of I is nilpotent. We say I is *nilpotent* if $I^n = 0$ for some $n \in \mathbb{N}$.[19]

Remark 103. Nilpotent left ideals are nil, but nil left ideals are not necessarily nilpotent.

Example 104. Let k be a field, and set $R = k[x_1, x_2, x_3, \ldots]/(x_1^2, x_2^3, x_3^4, \ldots)$. Then the ideal $(x_1, x_2, \ldots)$ is nil, but not nilpotent.

Remark 105. In the commutative case, the sum of two nilpotent elements is nilpotent. Indeed, if $x^n = y^m = 0$, then $(x+y)^{m+n-1} = 0$.[20] This tells us that the set of nilpotent elements form an ideal. However, this fails if R is non-commutative. Indeed in $M_2(\mathbb{Z})$ we have that if $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, then $A^2 = B^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. However, $A + B$ is a unit. Indeed, $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $(A+B)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This is because the left ideal generated by A contains non-nilpotent elements.

Exercise. A finite sum of nilpotent left ideals is nilpotent.

Conjecture. The sum of two nil left ideals is nil.

2.14.3 Wedderburn Radical

Definition 106. Let R be a ring. The *Wedderburn radical of R* (if it exists), denoted $W(R)$, is defined to be the largest nilpotent left ideal of R.[21]

Proposition 107. *Every nil left ideal is contained in $J(R)$.*

Proof. Let I be a nil left ideal, $y \in I$, and $x \in R$. Then $xy \in I$ and hence is nilpotent. Note that if u is nilpotent with $u^n = 0$, then $(1-u)^{-1} = 1+u+u^2+\ldots+u^{n-1}$. Thus, since xy is nilpotent, then $1-xy$ is a unit and hence $y \in J(R)$. □

Corollary 108. *It is immediate that when $W(R)$ exists, it is contained in $J(R)$.*

Theorem 109. *If R is a left (or right) Artinain ring, then $J(R)$ is nilpotent.*

Proof. Let $J = J(R)$ and consider the descending chain $J \supseteq J^2 \supseteq \ldots$. Since R is left Artinian, there exists some k so that $J^k = J^{k+1} = I$. If we can show that $I = 0$, then we'll have that $J(R)$ is nilpotent. Suppose not. Then consider the set $\Lambda = \{L \mid L \text{ is a left ideal and } IL \neq 0\}$. As we're assuming $I \neq 0$, then $R \in \Lambda$ so that $\Lambda \neq \emptyset$. Since R is Artinian, there is some $L \in \Lambda$ which is minimal. Since we have $IL \neq 0$ then there exists some $y \in L$ such that $Iy \neq 0$. As Iy is a left ideal, we must have $Iy \subseteq L$, since $I(Iy) = I^2y = Iy \neq 0$. Hence, $Iy \in \Lambda$ and $Iy \subseteq L$ which means by the minimality of L that $Iy = L$. Now, we get that $y = iy$ for some $i \in I$. Thus, $(1-i)y = 0$ but $i \in I \subseteq J$ so that $1 - i$ is a unit, and hence $y = 0$. This is a contradiction as we couldn't have had that $y = 0$ and so we must have that $I = 0$. □

Corollary 110. *It is immediate that for left (or right) Artinian rings, R, then $W(R)$ exists.*

2.15 Monday 13 February 2012

2.15.1 Artinian rings are Noetherain

Lemma 111. *Let R be a semisimple ring, and M an $R-$module. The following are equivalent:*

1. *M is finitely generated,*
2. *M is Artinian,*
3. *M is Noetherian, and*
4. *$\lambda_R(M) < \infty$.*

Proof. Since free modules over a semisimple ring are semisimple and quotients of semisimple modules are semisimple, then any module over a semisimple ring is semisimple. Hence, we have that $M = \bigoplus_{j \in \Lambda} I_j$ where each I_j is simple. Note that $|\Lambda| < \infty$ if and only if M has a composition series, which is true if and only if $\lambda_R(M) < \infty$ which is true if and only if M is both Noetherian and Artinian. Also, as R is both Noetherian and Artinian, then if M is finitely generated, we have that M is both Noetherian and Artinian. □

[19] Recall here that I^n is the left ideal generated by product of n elements from I, i.e. element of the form $\sum_{j=1}^{m} a_{j1} \ldots a_{jn}$ where $a_j i \in I$.

[20] This can be easily seen by writing out the product using the binomial coefficients since each term of the sum will have either x^n or y^m as a factor.

[21] That is, it contains all nilpotent left ideals, and $W(R)$ is nilpotent.

Remark 112. If M is an $R-$module, and I is an ideal of R such that $IM = 0$, then M is naturally an $R/I-$module by setting $\overline{r}m = rm$ for any $\overline{r} \in R/I$.

Note. If I is an ideal, and $I \subseteq J(R)$, then $J(R/I) = J(R)/I$. In particular, $J(R/J(R)) = 0$.

Theorem 113. *If R is a left Artinian ring, then R is left Noetherian.*

Proof. Let $J = J(R)$. Since R is left Artinian, then $J^n = 0$ for some n. Also, $J(R/J) = 0$, and R/J is left Artinian. Thus, R/J is semisimple by Proposition 101. If $\lambda_R(R/J^i) < \infty$ for all i, then $\lambda_R({}_RR) = \lambda_R(R/0) = \lambda_R(R/J^n) < \infty$ so that R is left Noetherian as well. We'll prove now that $\lambda_R(R/J^i) < \infty$ for all i by induction. Note that since R/J is Artinian, then by Lemma 111, we have $\lambda_R(R/J) < \infty$ which takes care of the base case. Suppose now that $\lambda_R(R/J^{i-1}) < \infty$ for some $i > 1$, and consider the module J^{i-1}/J^i. Since J^{i-1} is an ideal of R, then it is left Artinian as an $R-$module and hence J^{i-1}/J^i is left Artinian. Also, J^{i-1}/J^i is an $R/J-$module and is Artinian as an $R/J-$module. By Lemma 111, we then have that $\lambda_R(J^{i-1}/J^i) = \lambda_{R/J}(J^{i-1}/J^i) < \infty$. Now, consider the short exact sequence

$$0 \to J^{i-1}/J^i \to R/J^i \to R/J^{i-1} \to 0$$

where the maps are the obvious choices. Then $\lambda_R(R/J^i) = \lambda_R(J^{i-1}/J^i) + \lambda_R(R/J^{i-1}) < \infty$ and hence we get the desired result. □

2.15.2 Commutative Algebra

Definition 114. Let R be a commutative ring. An ideal $P \neq R$ is *prime* if whenever $ab \in P$ then $a \in P$ or $b \in P$. Equivalently, P is prime if and only if R/P is a domain.

Definition 115. Let R be a commutative ring, and $0 \notin S \subset R$. We say S is *multiplicatively closed* if $s_1 s_2 \in S$ whenever $s_1, s_2 \in S$. For convenience, we usually assume $1 \in S$.

Example 116. There are two main examples of multiplicatively closed sets:

1. If P is a prime ideal, then $R \setminus P$ is multiplicatively closed.
2. If $x \in R \setminus \{0\}$, the $S = \{x^n \mid n \geq 0\}$ is a multiplicatively closed set.

Proposition 117. *Let R be a commutative ring, $S \neq \emptyset$ a multiplicatively closed set of R with $0 \notin S$. Then there is a prime ideal P of R such that $P \cap S = \emptyset$.*

Proof. Let $\Lambda = \{I \mid I \text{ is an ideal of } R, \text{ and } I \cap S = \emptyset\}$. Note that $(0) \in \Lambda$ so that $\Lambda \neq \emptyset$. By Zorn's lemma, there exists a maximal element of Λ, say P. We need to show that P is prime. Note that $P \neq R$ as $S \neq \emptyset$, and suppose that P is not prime. Then there exist elements $a, b \in R \setminus P$ such that $ab \in P$. Then we have $(P, a) = P + Ra \supsetneq P$ and $(P, b) \supsetneq P$. Hence, $(P, a) \cap S \neq \emptyset$ and $(P, b) \cap S \neq \emptyset$. Let $s_1 = x_1 + r_1 a$ and $s_2 = x_2 + r_2 b$ where $x_i \in P$ and $r_i \in R$ for $i = 1, 2$. Then $s_1 s_2 = (x_1 + r_1 a)(x_2 + r_2 b) = x_1 x_2 + x_1 r_2 b + x_2 r_1 a + r_1 r_2 ab \in P$ so that $P \cap S \neq \emptyset$. This is a contradiction and so we must have that P is prime. □

Theorem 118 (Krull). *Let R be a commutative ring. Let* $\text{Nilrad}(R) = \{r \in R \mid r^n = 0 \text{ for some } n\} = \sqrt{(0)}$. *Then,* $\text{Nilrad}(R) = \bigcap P$ *where the intersection is taken over all prime ideals of R.*

Proof. ($\subseteq$) Let $r \in \sqrt{(0)}$ and P be a prime ideal. Then $r^n = 0 \in P$ for some n and hence $r \in P$ as P is prime.
($\supseteq$) Suppose that $r \notin \sqrt{(0)}$, and let $S = \{r^n \mid n \geq 0\}$ so that $0 \notin S$ and S is multiplicatively closed. Then by Proposition 117, there exists some prime ideal P such that $P \cap S = \emptyset$ and hence $r \notin P$. □

2.16 Wednesday 15 February 2012

2.16.1 History and Applications of Artin-Wedderburn

Note. We discussed some history of algebra in class today, but it seems not worth typing up. The dates in question were 1843-1965, but as was said in class..."History goes on." –T.M.

Theorem 119. *Let R be a simple, left Artinian ring. Then $R \cong M_n(D)$ for some division ring D.*

Proof. Let M be a simple left $R-$module, and let $D = R'(M) = \text{End}_R(M)$ which is a division ring. Now, consider the map $\lambda : R \to R''(E) = \text{End}_D(M)$. It is clear that $\ker(\lambda) = \text{Ann}_R(M)$ which is a 2-sided ideal and so $\ker(\lambda) = (0)$. If we can show that M is finitely generated over D, then we'll have that λ is surjective by Corollary 75. Suppose that $\dim_D(M) = \infty$. Then choose $\{e_1, e_2, \ldots\}$ to be a countable $D-$linearly independent set in M. Let $I_n = \{r \in R \mid re_i = 0 \text{ for } i = 1, \ldots, n\}$ and note that I_n is a left ideal of R with $I_n \supseteq I_{n+1}$ for each n. Also, for each n, there exists an $f \in \text{End}_D(M)$ such that $f(e_i) = 0$ for $i = 1, \ldots, n$ but $f(e_{n+1}) \neq 0$. By the Jacobsen Density Theorem (Theorem 74), there is some $r \in R$ such that $f(e_i) = re_i$ for $i = 1, \ldots, n+1$. This gives that $r \in I_n \setminus I_{n+1}$ so that the containment is always strict. This violates the fact that R is left Artinian, and so we must have that $\dim_D(M) < \infty$. This means that $M \cong D^n$ for some n and λ is an isomorphism. Hence, $R \cong \text{End}_D(D^n) \cong M_n(D^{op})$ and since D^{op} is a division ring whenever D is, that completes the proof. □

Theorem 120 (Special Case of Wedderburn's Theorem). *Let R be a finite dimensional $k-$algebra, where k is an algebraically closed field. Then R is semisimple if and only if $R \cong M_{n_1}(k) \times \ldots \times M_{n_\ell}(k)$.*

Proof. ($\Leftarrow$) This direction is clear by Example 53.
($\Rightarrow$) Since R is semisimple, then by Artin-Wedderburn (Theorem 55) we have that $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_\ell}(D_\ell)$, where each $D_i = \mathrm{End}_R(E_i)$ where $E_1, \ldots, E_\ell$ are the distinct up to isomorphism left simple modules of R. Since $\dim_k(R) < \infty$, then $E_i = Rx_i$ for any $x_i \in E_i \setminus \{0\}$ so that $\dim_k(E_i) < \infty$. Also, it is clear that $D_i = \mathrm{End}_R(E_i) \subseteq \mathrm{End}_k(E_i) \cong M_n(k)$ where $n = \dim_k(E_i)$. Thus, $\dim_k(D_i) < \infty$ for all i. Let $\alpha_i \in D_i$. Then $k[\alpha_i]$ is a finite dimensional $k-$vector space, and also a commutative domain. Hence, $k[\alpha_i] = k$ since k is algebraically closed, and so $D_i = k$ for all i. □

2.16.2 Commutative Algebra

Remark 121. For the time being, R will be a commutative ring.

Definition 122. Let I be an ideal of R. A prime ideal P of R is said to be *minimal over* I if $I \subseteq P$ and whenever Q is also prime with $I \subseteq Q \subseteq P$ then $P = Q$.

Remark 123. By Zorn's lemma, every ideal $I \neq R$ has a prime minimal over it.

Notation. We set $\mathrm{Spec}(R) = \{P \mid P \text{ is a prime ideal of R}\}$ and $\min_R(R/I) = \{P \in \mathrm{Spec}(R) \mid P \text{ is minimal over } I\}$.

Definition 124. If $P \in \mathrm{Spec}(R)$, then the *height of* P is

$$\mathrm{ht}(P) = \sup\{n \mid \text{ there exists a chain of primes } P = P_n \supsetneq P_{n-1} \supsetneq \ldots \supsetneq P_0\}.$$

Also, the *dimension of a ring* R is $\dim R = \sup\{\mathrm{ht}(P) \mid P \in \mathrm{Spec}(R)\}$.

Example 125. Let F be a field.

1. $\dim(F) = 0$ since $\mathrm{Spec}(F) = \{(0)\}$.
2. $\dim(F[x]) = 1$ since $\mathrm{Spec}(F[x]) = \{(0), (f) \mid f \text{ is irreducible }\}$.
3. $\dim(\mathbb{Z}) = 1$ since $\mathrm{Spec}(\mathbb{Z}) = \{(0), (p) \mid p \text{ is prime }\}$.
4. $\dim(\mathbb{Z}/(6)) = 0$ since $\mathrm{Spec}(\mathbb{Z}/(6)) = \{(\overline{2}), (\overline{3})\}$.

Remark 126. We have $\dim(R) = 0$ if and only if every prime of R is minimal over (0) which is true if and only if every prime of R is maximal over (0).

2.17 Friday 17 February 2012

2.17.1 More Commutative Algebra

Definition 127. If I is an ideal, then the *radical of* I is $\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n\}$.

Exercise. $\sqrt{I} = \bigcap P$ where the intersection is taken over all primes $P \in \min_R(R/I)$.

Fact. If R is Noetherian, then $\mathrm{ht}(P) < \infty$ for all $P \in \mathrm{Spec}(R)$, however, there exist Noetherian rings with $\dim(R) = \infty$.

Exercise. If $P \in \mathrm{Spec}(R)$, and $P \supseteq I_1 I_2 \ldots I_n$, then $P \supseteq I_j$ for some j.

Proposition 128. *Let R be Noetherian. Then $\min_R(R/I)$ is a finite set for every ideal I of R.*

Proof. Suppose not, and consider the set $\Lambda = \{I \mid \min_R(R/I) \text{ is an infinite set}\}$. Since R is Noetherian, and $\lambda \neq \emptyset$, then there exists a maximal element of Λ, say I. Since $\min_R(R/I)$ is an infinite set, then $P \notin \mathrm{Spec}(R)$. Thus, there exist some $a, b \in R \setminus I$ such that $ab \in I$. Let $J_1 = (I, a) = I + Ra$ and $J_2 = (I, b)$. Note that $J_1, J_2 \supsetneq I$. Thus, by the maximality of I, we have that $\min_R(R/J_i)$ is finite for $i = 1, 2$. But $J_1 J_2 \subseteq I$ since $(i_1 + r_1 a)(i_2 + r_2 b) = i_1 i_2 + r_1 a i_2 + r_2 b i_1 + r_1 r_1 ab \in I$ for all $i_1, i_2 \in I$ and $r_1, r_2 \in R$. Let $P \in \mathrm{Spec}(R)$. Then $P \supseteq I$ if and only if $P \supseteq J_1$ or $P \supseteq J_2$ so $\min_R(R/I) \subseteq \min_R(R/J_1) \cup \min_R(R/J_2)$ which is a contradiction, and so we must have that $\min_R(R/I)$ is a finite set for every ideal I of R. □

Theorem 129. *Let R be a commutative ring. The following are equivalent:*

1. *R is Artinian, and*
2. *R is Noetherian with $\dim(R) = 0$.*

Proof. ($1 \Rightarrow 2$) We've already shown that since R is Artinian, then R is Noetherian in Theorem 113. So we claim first that R has only finitely many maximal ideals. If not, then we can let $\{m_1, m_2, \ldots\}$ be an infinite set of distinct maximal ideals of R. By considering the descending chain $m_1 \supseteq (m_1 \cap m_2) \supseteq (m_1 \cap m_2 \cap m_3) \supseteq \ldots$ we see that $m_1 \cap \ldots \cap m_i = m_1 \cap \ldots \cap m_{i+1}$ for some i. Thus, $m_{i+1} \supseteq m_1 \cap \ldots \cap m_i \supseteq m_1 m_2 \ldots m_i$. Since m_{i+1} is maximal, then it is also prime, and so for some $j \in \{1, \ldots, i\}$ we have $m_j \subseteq m_{i+1}$ by maximality of m_j this means that $m_j = m_{i+1}$ which

contradicts the choice of the set of maximal ideals. Thus, R has only finitely many maximal ideals. Now, we've shown in Theorem 109 that since R is Artinian, then $J(R)$ is nilpotent, say $J(R)^n = 0$. Also, we have that $J(R) = \bigcap_{i=1}^t m_i$ where $\{m_i\}_{i=1}^t$ is all of the maximal ideals of R. Then, $m_1^n m_2^n \dots m_t^n \subseteq \cap_{i=1}^t m_i^n = J(R)^n = 0$, and so for any $P \in \text{Spec}(R)$, we have $P \supseteq m_1^n \dots m_t^n$ and hence $P \supseteq m_r$ for some r. Thus, every prime is maximal and so $\dim(R) = 0$.
$(2 \Rightarrow 1)$ As R is Noetherian, then by Theorem 128, we have $\text{Spec}(R) = \min_R(R) = \min_R(R/(0)) = \{P_1, \dots, P_t\}$. Thus, $J = J(R) = \cap_{i=1}^t P_i = \sqrt{(0)}$. Since R is Noetherian, then J is finitely generated, and each element of $J(R) = \sqrt{(0)}$ is nilpotent, by definition of $\sqrt{(0)}$. Then because J is finitely generated, we can let n be the maximal power needed to get each generator of J to be zero, and then $J^n = 0$ follows so that J is nilpotent. We now claim that $\lambda_R(R/J^i) < \infty$ for all i, which would imply that R is Artinian. So, when $i = 1$, we have that $R/J = R/(P_1 \cap \dots \cap P_t) = R/P_1 \times \dots \times R/P_t$ by the Chinese Remainder Theorem since $m_i + m_j = R$ for all $i \neq j$. Thus, R/J is semisimple by Artin-Wedderburn, and hence $\lambda_{R/J}(R/J) = \lambda_R(R/J) < \infty$ by Proposition 56. For the inductive step, suppose that $\lambda_R(R/J^{i-1}) < \infty$. Then J^{i-1}/J^i is an $R/J-$module, and as R is Noetherian, then J^{i-1} is Noetherian, and hence J^{i-1}/J^i is Noetherian as an $R/J-$module. Since R/J is semisimple, then $\lambda_R(J^{i-1}/J^i) = \lambda_{R/J}(J^{i-1}/J^i) < \infty$ by Lemma 111. Then, the short exact sequence:

$$0 \to J^{i-1}/J^i \to R/J^i \to R/J^{i-1} \to 0$$

gives us that $\lambda_R(R/J^i) = \lambda_R(J^{i-1}/J^i) + \lambda_R(R/J^{i-1}) < \infty$. Thus, $\lambda_R(R) = \lambda_R(R/(0)) = \lambda_R(R/J^n) < \infty$ by Proposition 42. □

Note. If R is any commutative ring, then $\text{Spec}(R/I) = \{P/I \mid P \in \text{Spec}(R), P \supseteq I\}$. Also, $P/I = Q/I$ if and only if $P = Q$.

Example 130. Let k be a field.

1. If $R = k[x,y,z]/(x^3, y^3, z^3)$ then R is Notherian by the Hilbert Basis Theorem. Also, $\text{Spec}(R) = \{(x,y,z)\}$ so $\dim(R) = 0$, and R is Artinian.
2. If $R = \mathbb{Z}[x]/(12, x^3 - x)$, then R is Noetherian by the Hilbert Basis Theorem. Also,

$$\text{Spec}(R) = \left\{ \frac{(2,x)}{(12,x^3-x)}, \frac{(3,x)}{(12,x^3-x)}, \frac{(2,x-1)}{(12,x^3-x)}, \frac{(3,x-1)}{(12,x^3-x)}, \frac{(2,x+1)}{(12,x^3-x)}, \frac{(3,x+1)}{(12,x^3-x)} \right\}$$

and so $\dim(R) = 0$ and R is Artinian.

2.18 Wednesday 22 February 2012

2.18.1 Modules over Artinian ring

Proposition 131. [22] *Let R be a left Artinian ring, and M a left $R-$module. The following are equivalent:*

1. *M is finitely generated,*
2. *M is Noetherian,*
3. *M is Artinian,*
4. *$\lambda_R(M) < \infty$.*

Proof. $(4 \Rightarrow 2)$ This is true by Proposition 42.
$(2 \Rightarrow 1)$ This is clear by definition of Noetherian modules.[23]
$(1 \Rightarrow 3)$ Finitely generated modules over an Artinian ring are all Artinian, since they're isomorphic to a quotient of a free module.
$(3 \Rightarrow 4)$ Let $J = J(R)$. Then $J^n = 0$ for some n by Theorem 109 since R is Artinian. Also, R/J is semisimple by the same argument as in part two of the proof of Theorem 129. We then claim that $\lambda_R(M/J^iM) < \infty$ for all $i \geq 1$. For the base case, we know that M/JM is an $R/J-$module and since M is Artinian, then M/JM is Artinian and so by we have that $\lambda_R(M/JM) = \lambda_{R/J}(M/JM) < \infty$ by Lemma 111. So consider the $R/J-$module $J^{i-1}M/J^iM$. This module is also Artinian, and so $\lambda_{R/J}(J^{i-1}M/J^iM) < \infty$ by Lemma 111. Then the additivity of length on exact sequences gives that $\lambda_R(M/J^iM) < \infty$ for all i since $0 \to J^{i-1}M/J^iM \to M/J^iM \to M/J^{i-1}M \to 0$ is an exact sequence. Thus, $\lambda_R(M) = \lambda_R(M/(0)) = \lambda_R(M/J^nM) < \infty$. □

[22] Tom was sick on Monday 20 February 2012.
[23] Or by Proposition 3 if you're so inclined.

Chapter 3

Exam 2 Material

3.1 Wednesday 22 February 2012

3.1.1 Split Exact Sequences

Proposition 132. *Let R be a ring and*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

a short exact sequence of left $R-$modules. The following are equivalent:

1. *There is an $R-$module homomorphism $j : C \to B$ such that $gj = 1_C$.*
2. *There is an $R-$module homomorphism $i : B \to A$ such that $if = 1_A$.*
3. *There are $R-$module homomorphisms $i : B \to A$ and $j : C \to B$ such that $1_B = fi + jg$.*

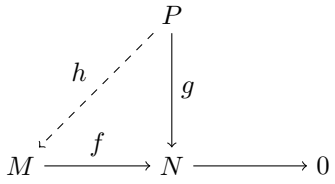
Proof. First note that $gf = 0$ since the sequence is exact. Also, recall that when g is surjective, then $\alpha g = \beta g$ implies that $\alpha = \beta$. This is a consequence of surjective maps being epimorphisms in the category of sets. Also, when f is injective then $f\alpha = f\beta$ implies that $\alpha = \beta$ because injective maps are monomorphisms in the category of sets. For a reminder of what epimorphisms and monomorphisms are, see 901 notes page 2.
$(3 \Rightarrow 1)$ By the hypothesis here, we have that $1_B = fi + jg$. Composing with g on the left (i.e. as the last map applied) gives $1_C g = g = gfi + gjg = gjg$ since $gf = 0$. Hence we get that $1_C = gj$ because g is surjective.
$(1 \Rightarrow 2)$ Let $K = \ker(g) = \text{image}(f) \cong A$. Also, let $\rho : K \to A$ be an isomorphism given by $\rho(k) = f^{-1}(k)$. Also, let $b \in B$ and note that $g(b - jg(b)) = g(b) - gjg(b) = g(b) - g(b) = 0$ so $b - jg(b) \in K$. Now, $1_B - jg : B \to K$ is an $R-$module homomorphism. Let $i : B \to A$ be defined by $\rho \circ (1_B - jg)$. Then, $if = \rho(1 - jg)f = \rho f - \rho jgf = \rho f = 1_A$ since $gf = 0$.
$(2 \Rightarrow 3)$ Define $j : C \to B$ by $j(g(b)) = b - fi(b)$. Since g is surjective, then every element $c \in C$ is of the form $g(b)$ for some $b \in B$, so this definition actually makes sense as long as we can show that it is well defined. So suppose that $g(b) = g(b')$. Then, $b - b' \in \ker(g) = \text{image}(f)$, and we can choose $\alpha \in A$ so that $b - b' = f(\alpha)$. Then $j(g(b)) - j(g(b')) = g(b - b') = b - b' - fi(b - b') = b - b' - fi(f(\alpha) = b - b'f(\alpha) = 0$ since $if = 1_A$ and hence j is well defined. Now, $(fi + jg)(b) = fi(b) + jg(b) = fi(b) + b - fi(b) = b$ so that we have $fi + jg = 1_B$ as desired. □

Definition 133. A short exact sequence is *split* if it satisfies the equivalent conditions in the previous proposition. Moreover, when this happens, $B \cong A \oplus C$.

3.2 Friday 24 February 2012

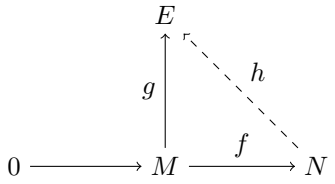
3.2.1 Projective Modules

Definition 134. An $R-$module, P, is called *projective* if given any diagram of the form below (with exact row),



then there exists a map $h : P \to M$ such that the diagram commutes.

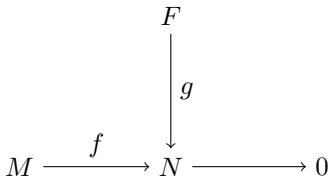
Definition 135. An $R-$module, E, is called *injective* if given any diagram of the form below (with exact row),



then there exists a map $h : N \to E$ such that the diagram commutes.

Proposition 136. *Any free module is projective.*

Proof. Let F be a free $R-$module, and consider any diagram of the form below with exact row where M and N are $R-$modules.

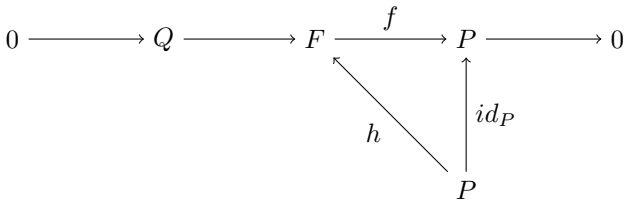


Let S be a basis for F. For each $x \in S$, choose $m_x \in M$ so that $f(m_x) = g(x)$. Note that this is possible since f is surjective. Then, define a map $h : F \to M$ by setting $h(x) = m_x$ for all $x \in S$. Then we have that $fh = g$ by construction, and so F is projective. □

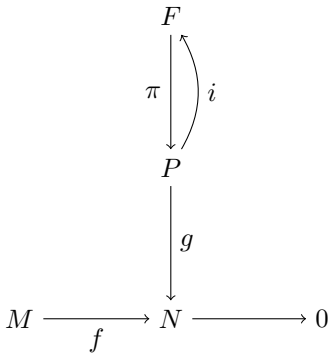
Proposition 137. *Let P be an $R-$module. The following are equivalent:*

1. *P is projective, and*
2. *there exists an $R-$module, Q, such that $P \oplus Q$ is a free $R-$module.*

Proof. $(1 \Rightarrow 2)$ Note that any $R-$module is the homomorphic image of a free module. So let F be a free $R-$module such that there exists a surjective map $f : F \to P$. Let $Q = \ker(f)$. Then the sequence $0 \to Q \to F \to P \to 0$ is exact. Since P is projective, there exists a map $h : P \to F$ such that the diagram below commutes.



Thus, $fh = id_P$, meaning that the sequence splits, and hence $F \cong P \oplus Q$.
$(2 \Rightarrow 1)$ Now, suppose that $P \oplus Q \cong F$ where F is a free $R-$module. Let $\pi : F \to P$ be the usual projection map, and $i : P \to F$ the usual injection so that $\pi i = id_P$. Consider the diagram below where M and N are any $R-$modules, and the row is exact.



Since F is projective, there is a map $\widetilde{h} : F \to M$ such that $f\widetilde{h} = g\pi$. Thus, $f\widetilde{h}i = g\pi i = g$ so that the map $h = \widetilde{h}i$ will give $fh = g$. □

Example 138. Let $R = \mathbb{Z}/(6) \cong (\overline{2}) \oplus (\overline{3})$ so that $(\overline{2})$ and $(\overline{3})$ are projective $R-$modules, but are not free $R-$modules.

Exercise. Let R be a commutative ring, and I an ideal of R. Then I is free if and only if $I = 0$ or $I = (a)$ for some non-zerodivisor $a \in R$.

Example 139. Let $R = M_n(D)$ for some division ring D, and let I be the matrices whose only nonzero entries are in the first row. Note that I is then an ideal of R and that $R = I \oplus J$ where J is the matrices whose first row is all zero. Thus, both I and J are projective, but neither is free. Note here that $n = \dim_D(I) < \dim_D(R) = n^2$ and $n(n-1) = \dim_D(J) < \dim_D(R) = n^2$.

Remark 140. 1. Let $R = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1+\sqrt{-5})$. Then I is projective, but not free.
2. A ring R is a PID if and only if every ideal is free.
3. Let R be a commutative ring, and e a nontrivial idempotent. Then $R = Re \oplus R(1-e)$ so that Re and $R(1-e)$ are projective but not free.
4. Let $S = \mathbb{R}[x,y,z]/(x^2+y^2+z^2-1)$ and define $\phi : S^3 \to S$ via $(a,b,c) \longmapsto \overline{x}a + \overline{y}b + \overline{z}c$. Let $K = \ker(\phi)$. Note that ϕ is surjective since $\phi(\overline{x}, \overline{y}, \overline{z}) = \overline{x}^2 + \overline{y}^2 + \overline{z}^2 = \overline{1}$. Then the diagram below is commutative with exact row so that the sequence splits, and $K \oplus S \cong S^3$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & S^3 & \xrightarrow{f} & S & \longrightarrow & 0 \\ & & & & & \nwarrow & \uparrow{\scriptstyle id_S} & & \\ & & & & & & S & & \end{array}$$

Thus K is a projective $S-$module, but it is not free.[1]
5. In 1955, Serre asked if there exist non-free projective modules over $k[x_1, \ldots, x_n]$ where k is a field. The answer is no, and was proved by Quillen-Suslin in the mid 1970's.

3.3 Monday 27 February 2012 & Wednesday 29 February 2012

3.3.1 Exam Review

Note. For most of these two days we reviewed for the exam. I'm not typing up all that was said, but I'm not skipping any new material.

Theorem 141. *Let R be a ring, and M a semisimple module. The following are equivalent:*
1. *M is finitely generated,*
2. *$\lambda_R(M) < \infty$,*
3. *M is Artinian,*
4. *M is Noetherian, and*
5. *$M = E_1 \oplus \ldots \oplus E_s$ where each E_i is simple.*

3.4 Wednesday 29 February 2012

3.4.1 Projective Modules

Proposition 142. *Let R be a ring. The following are equivalent:*
1. *R is semisimple, and*
2. *every $R-$module is projective.*

Proof. $(1 \Rightarrow 2)$ Let M be an $R-$module and $\phi : F \to M$ a surjective module homomorphism where F is a free module. Then the sequence below is exact where $K = \ker(\phi)$.

$$0 \longrightarrow K \xrightarrow{i} F \xrightarrow{\phi} M \longrightarrow 0$$

Since R is semisimple, F is also semisimple, and so $F = K \oplus N$ for some $R-$module, N. Thus, there exists a map $\pi : F \to K$ such that $\pi(x) = x$ for all $x \in K$. Hence, the sequence splits, $F \cong K \oplus M$ and hence M is projective.
$(2 \Rightarrow 1)$ Now, let I be an ideal of R and consider the short exact sequence $0 \to I \to R \to R/I \to 0$. This sequence splits since R/I is projective, and so the map $i : I \to R$ splits, meaning that I is a direct summand of R and hence R is semisimple. □

Fact. If k is a field, then every projective module of $k[x_1, \ldots, x_n]$ is free.

Definition 143. A projective module, P, is called *stably free* if $P \oplus R^n \cong R^m$ for some $n, m \in \mathbb{N}$. Here, the rank of P is $m - n$.

Fact. In the early 1970s, Suslin proved the following statement: Let R be a smooth finitely generated $k-$algebra, where k is an algebraically closed field of dimension d and characteristic 0. If P is a stably free projective of rank $\geq d$, then P is free.[2]

Fact. There exist stably free projective modules of rank $d-2$ which are not free. This was proved by Murthy.

Fact. In 2011, Jean Fasel[3] proved something about the rank $d-1$ case.[4]

[1] This is HARD to show!
[2] This must be that the dimension of R is d, since there are no nonzero prime ideals in a field, and we aren't talking about vector space dimension either. My notes are unclear on this.
[3] Who interviewed recently for the tenure-track job.
[4] Tom was unspecific about exactly what he proved, and I believe we were running out of time, so I just scribbled something down and left.

3.5 Friday 2 March 2012

3.5.1 von Neumann Regular Rings

Definition 144. A ring, R, is called *von Neumann regular* if for every $a \in R$ there is some $x \in R$ such that $axa = a$.

Example 145. 1. Any division ring is von Neumann regular.
2. Products of von Neumann regular rings are von Neumann regular.[5]
3. Arbitrary products of division rings are von Neumann regular.
4. If R is a von Neumann regular ring, and I is an ideal of R, then R/I is von Neumann regular as well.[6]
5. Let F be a field, and take Λ to be an infinite set. Let $R = \prod_{i\in\Lambda} F$, and let $I = \oplus_{i\in\Lambda} F$. Note that I is an ideal of R, and R is von Neumann regular, so R/I is von Neumann regular, but we showed in the homework that R/I is not a product of fields.

Proposition 146. *Let R be a ring. The following are equivalent:*

1. R is von Neumann regular,
2. every finitely generated left ideal of R is generated by an idempotent, and
3. every finitely generated left ideal of R is a direct summand of R.

Proof. $(2 \Rightarrow 3)$ Let I be a finitely generated left ideal of R. Then $I = Re$ by assumption, where $e^2 = e$. Then $R = Re \oplus R(1-e) = I \oplus R(1-e)$ so that I is a direct summand of R as desired.
$(3 \Rightarrow 1)$ Let $a \in R$. Then by assumption, $R = Ra \oplus J$ for some left ideal J of R. Let $1 = ra + j$ for some $r \in R$ and $j \in J$. Then $a = ara + aj$, so that $aj = a - ara \in Ra \cap J$ and hence $aj = 0$ and $a = ara$ so that R is von Neumann regular.
$(1 \Rightarrow 2)$ For this direction we induct on the number of generators of I, which we'll denote by n. For $n = 1$, we have that $I = Ra$. Then there exists some $x \in R$ such that $axa = a$ since R is von Neumann regular. Set $e = xa$. We have that $e^2 = xaxa = xa = e$ so that e is an idempotent. We clearly have $Re \subseteq Ra$. Also, $a = axa = ae \in Re$ so $Re = Ra = I$ and I is generated by an idempotent. Now suppose that $n > 1$ and we have $I = Ra_1 + \ldots + Ra_n$. By induction, there exist idempotents e_1, and e_2 such that $Ra_1 + \ldots + Ra_{n-1} = Re_1$ and $Ra_n = Re_2$. So we have that $I = Re_1 + Re_2$. Note that $I = Re_1 + Re_2 = Re_1 + Re_2(1-e_1)$ since $e_2 = e_2e_1 + 1e_2(1-e_1)$ and $e_2(1-e_1) = -e_2e_1 + 1e_2$. Now, by the $n = 1$ case, there is an idempotent $f \in R$ such that $Rf = Re_2(1-e_1)$. This gives that $I = Re_1 + Rf$. Note that $fe_1 = 0$ since $f = re_2(1-e_1)$ for some $r \in R$ so that $fe_1 = re_2(1-e_1)e_1 = 0$. Thus, $f(f+e_1) = f^2 + fe_1 = f^2 = f$. Now, since $f, e_1 \in I$, then $R(f+e_1) \subseteq I$. Also, $f = f(f+e_1) \in R(f+e_1)$ so that $e_1 = f + e_1 - f \in R(f+e_1)$ and hence $I = Re_1 + Rf \subseteq R(f+e_1)$ and hence we're done by the $n = 1$ case. □

Corollary 147. *Let R be a ring. The following are equivalent:*

1. R is semisimple, and
2. R is von Neumann regular and left Noetherian.

Proof. $(1 \Rightarrow 2)$ We know that semisimple rings are left Noetherian, so let I be a (finitely generated)[7] left ideal of R. Then I is a direct summand of R since R is semisimple. By proposition 146, R is von Neumann regular.
$(2 \Rightarrow 1)$ Let I be a left ideal of R. Then I is finitely generated since R is left Noetherian. By proposition 146, I is a direct summand of R, so R is semisimple. □

Note. Since semisimple was equivalent to semiprimitive and left Artinian (see proposition 101), then a ring is von Neumann regular and left Noetherian if and only if it is semiprimitive and left Artinian.

3.5.2 Maschke's Theorem

Theorem 148 (Maschke's Theorem, 1899). *Let G be a finite group, and k a field. Then $R = k[G]$ is semisimple if and only if the characteristic of the field does not divide the order of the group (*$\mathrm{char}(k) \nmid |G|$*).*

Proof. $(\Rightarrow)$ We proceed by contrapositive, so suppose that $\mathrm{char}(k) \mid |G|$. Letting 1_k denote the identity of the field, k, we have that $|G| \cdot 1_k = 0$. Let $x = \sum_{g\in G} g \in k[G]$, and let $h \in G$. Then $hx = \sum_{g\in G} hg = \sum_{g\in G} g = x$ since as sets $hG = G$. Similarly, $xh = x$. Thus, $x \in Z(k[G])$. Note that $x^2 = x(\sum_{g\in G} g) = \sum_{g\in G} xg = \sum_{g\in G} x = |G| \cdot x = 0$. Thus, Rx is a nilpotent ideal and $Rx \neq 0$. Hence $Rx \subseteq J(R) \neq 0$ which by proposition 101 means that R is not semisimple.
$(\Leftarrow)$ Now, let I be a left ideal of $R = k[G]$. We need to show that I is a direct summand of R, and note that it is enough to show that the injective map $i : I \to R$ splits. So we want to find an $R-$module homomorphism $\rho : R \to I$ such that $\rho i = id_I$, that is, we need $\rho(a) = a$ for all $a \in I$. However, since I is a $k-$subspace of R, then there exists a $k-$linear map $\pi : R \to I$ which fixes I. As I is a left ideal of R, then for all $g \in G$, $g\pi g^{-1} : R \to I$ given by $r \longmapsto g \cdot \pi(g^{-1}r)$ is also $k-$linear. So define $\rho : R \to I$ by

$$\rho = \frac{1}{|G|} \sum_{g\in G} g\pi g^{-1}.$$

[5]This is shown by doing the obvious thing to try. Details are in my handwritten notes.
[6]This is shown by doing the obvious thing to try. Details are in my handwritten notes.
[7]All left ideals are finitely generated since R is left Noetherian.

We need to show ρ is $R-$linear, and that $\rho i = id_I$. We already have that ρ is $k-$linear, so it is enough to show that for all $h \in G$, and $a \in R$, that $\rho(ha) = h\rho(a)$. Indeed, we have

$$\begin{aligned}
\rho(ha) &= \frac{1}{|G|}\sum_{g\in G} g\pi g^{-1}(ha) \\
&= \frac{1}{|G|}\sum_{g\in G} g\pi((h^{-1}g)^{-1}a) \\
&= \frac{1}{|G|}\sum_{g\in G} h(h^{-1}g)\pi((h^{-1}g)^{-1}a) \\
&= \frac{1}{|G|}h\sum_{g\in G} g\pi g^{-1}(a) \\
&= h\rho(a)
\end{aligned}$$

since $h^{-1}G = G$ as sets. It remains then to show that for all $a \in I$ that $\rho(a) = a$. Recall that $\pi(a) = a$. then $g\pi g^{-1}(a) = g \cdot \pi(g^{-1}a) = gg^{-1}a = a$, so $\rho(a) = \frac{1}{|G|}\sum_{g\in G} g\pi g^{-1}(a) = \frac{1}{|G|}|G|a = a$. Hence, ρ is a splitting map for i, and hence I is a direct summand of R.[8] □

3.6 Monday 5 March 2012

3.6.1 Semisimple Algebras over a Field

Recall. Let R be a semisimple ring.

- ▷ If R is simple, then $R \cong nI = \underbrace{I \oplus \ldots \oplus I}_{\text{n copies}}$ where I is a simple left ideal. Also, if we set $D = \mathrm{End}_R(I)$, then $R \cong \mathrm{End}_D(I) = R''(I) = M_r(D^{op})$ where $r = \dim_D(I)$.
- ▷ In general, $R \cong n_1I_1 \oplus \ldots \oplus n_tI_t$ where each I_j is a simple left ideal, and $I_i \ncong I_j$ whenever $i \neq j$. On the homework, we introduced the notation that $B(I_j)$ is the sum off all left ideals isomorphic to I_j, that is, $B(I_j) = \sum_{J\cong I_j} J \cong n_jI_j$. Thus, we have that $R \cong B(I_1) \times \ldots \times B(I_t)$. Also, if we set $D_j = \mathrm{End}_R(I_j) = \mathrm{End}_{B(I_j)}(I_j)$, then $B(I_j) \cong \mathrm{End}_{D_j}(I_j)$ by the simple case. Note also that these expressions for R are unique up to isomorphism.

Theorem 149. *Let R be a semisimple ring which is also a finite dimensional $k-$algebra where k is an algebraically closed field. We write $R = n_1I_1 \oplus \ldots \oplus n_tI_t$ where $I_i \ncong I_j$ whenever $i \neq j$. Then,*

1. $\mathrm{End}_R(I_j) = k$,
2. $n_j = \dim_k(I_j)$, *and*
3. $\dim_k(R) = \sum_{j=1}^t n_j^2$.

Proof. 1. Let $D_j = \mathrm{End}_R(I_j)$, and note that this is a division ring. Also note that the map $k \to D_j$ given by $a \longmapsto \ell_a$ is an embedding since $k \subseteq Z(R)$, so that $\ell_a \in \mathrm{End}_R(I_j)$. So consider $k \subseteq \mathrm{End}_R(I_j) = D_j$. In fact, we have $k \subseteq Z(D_j)$ since for all $f \in \mathrm{End}_R(I_j)$, then $f \circ \ell_a = \ell_a \circ f$. We also have that $m_j = \dim_k(I_j) \leq \dim_k(R) < \infty$ and that $D_j = \mathrm{End}_R(I_j) \subseteq \mathrm{End}_k(I_j) \cong M_{m_j}(k)$. Thus, $\dim_k(D_j) \leq m_j^2 < \infty$. Let $\alpha \in D_j$. Then $k[\alpha]$ is a commutative domain which is finite dimensional over k. Thus, α is algebraic over k and so $\alpha \in k$ and $D_j = k$.

2. Now, $n_jI_j \cong B(I_j) = \mathrm{End}_{D_j}(I_j) = \mathrm{End}_k(I_j) \cong M_{m_j}(k)$. Taking dimensions of the two ends over k gives $n_jm_j = m_j^2$ and so we have $m_j = n_j$ as desired.

3. Now it is easy to see that $\dim_k(R) = \sum_{j=1}^t n_j \dim_k(I_j) = \sum_{j=1}^t n_j^2$.

□

Proposition 150. *Let G be a finite group, and k a field. Let $C_1, \ldots, C_r$ be the distinct conjugacy classes of G. For each i, let $z_i = \sum_{g\in C_i} g \in k[G]$. Then $\{z_i\}_{i=1}^r$ forms a $k-$basis for $Z(k[G])$.*

Proof. For any $g \in G$, and for any $i \in \{1, \ldots, r\}$, we clearly have $gC_ig^{-1} = C_i$. Thus, $gz_ig^{-1} = g(\sum_{h\in C_i} h)g^{-1} = \sum_{h\in C_i} ghg^{-1} = z_i$. Hence, $gz_i = z_ig$ for all $g \in G$, meaning that $z_i \in Z(k[G])$. Since $C_i \cap C_j = \emptyset$ whenever $i \neq j$ and the elements of G are linearly independent over k, we see that $\{z_1, \ldots, z_r\}$ is a linearly independent set over k. It remains so show that they span $Z(k[G])$. Let $x = \sum_{g\in G} a_gg \in Z(R)$ and let $h \in G$. Then $x = hxh^{-1} = \sum_{g\in G} a_ghgh^{-1} = \sum_{g\in G} a_{h^{-1}gh}g$. By the linear independence of the elements of G, we get that $a_g = a_{h^{-1}gh}$ for all $g \in G$ and $h \in H$. thus, if $g_1, g_2 \in C_i$ for some i, then $a_{g_1} = a_{g_2}$. So for each i, choose $g_i \in C_i$. Then, $x = \sum_{i=1}^r a_{g_1}z_i \in \mathrm{span}\{z_1, \ldots, z_r\}$ and so the set $\{z_1, \ldots, z_r\}$ forms a basis for $Z(k[G])$.[9] □

[8] Part of this proof was actually done in class on March 5th, but it is easiest to read when it is put into one day rather than split amongst more than one.

[9] Part of the proof was done on Wednesday, but as always, the proof reads easier if it is not broken up.

3.7 Wednesday 7 March 2012

3.7.1 Semisimple Group Rings

Recall. A field k is algebraically closed if and only if whenever F is a field, with $k \subseteq F$, and F is algebraic over k, then $F = k$.

Exercise. If $k \subseteq R$ where k is a field, R is a commutative domain, and $\dim_k(R) < \infty$, then R is a field, and R is algebraic over k.

Proposition 151. *Let $R = k[G]$, where G is a finite group, and k an algebraically closed field such that $\text{char}(k) \nmid |G|$. Then the number of conjugacy classes of G is the number of distinct simple left ideals of R.*

Proof. Let t be the number of distinct simple left ideals of R. Then $R = n_1 I_1 \oplus \ldots \oplus n_t I_t$ where each I_j is simple and $I_i \ncong I_j$ whenever $i \neq j$. We also have $R \cong B(I_1) \times \ldots \times B(I_t) \cong M_{n_1}(k) \times \ldots \times M_{n_t}(k)$ where $B(I_j) = \text{End}_k(I_j) = M_{n_j}(k)$ is simple and semisimple. Thus, $Z(R) = Z(M_{n_1}(k)) \times \ldots \times Z(M_{n_t}(k)) \cong k \cdot id_{n_1} \times \ldots \times k \cdot id_{n_t}$. Thus, $\dim_k(Z(R)) = \dim_k(k \cdot id_{n_1} \times \ldots \times k \cdot id_{n_t}) = t$ is the number of conjugacy classes by Proposition 150. □

Corollary 152 (Summary). *Let $R = k[G]$, where G is a finite group, and k an algebraically closed field such that $\text{char}(k) \nmid |G|$. Write $R = n_1 I_1 \oplus \ldots \oplus n_t I_t$ where each I_j is a simple left ideal and $I_i \ncong I_j$ whenever $i \neq j$. Then,*

1. *$n_j = \dim_k(I_j)$,*
2. *$k = \text{End}_R(I_j)$,*
3. *$\sum_{j=1}^{t} n_j^2 = |G|$, and*
4. *t is the number of conjugacy classes of G.*

Corollary 153. *Let $R = k[G]$, where G is a finite group, and k an algebraically closed field such that $\text{char}(k) \nmid |G|$. Then G is abelian if and only if $\dim_k(M) = 1$ for all simple left $R-$modules, M.*

Proof. G is abelian if and only if the number of conjugacy classes of G is $|G|$ so that $t = |G|$. This is true if and only if $n_j = 1$ for all j by corollary 152 which is true if and only if $\dim_k(I_j) = 1$ for all j. In turn, this is true if and only if $\dim_k(M) = 1$ for all simple left $R-$modules M since such an M will be congruent to I_j for some j. □

Example 154. Let $G = S_3$. Then, we know that $t = 3$. The conjugacy classes are: $\{(1)\}$, $\{(12), (13), (23)\}$, and $\{(123), (132)\}$. Also, we must have that $n_1^2 + n + 2^2 + n_3^2 = 6$ so we have $n_1 = n_2 = 1$ and $n_3 = 2$. This gives that $I_1 \cong k$, $I_2 \cong k$ as $k-$vector spaces, but notice that $I_1 \ncong I_2$ as $R-$modules. Also, $I_3 \cong k^2$. Our goal is to describe these better! And so we'll start studying representation theory to do this.

3.7.2 Starting Representation Theory

Idea. Whenever G acts on something, we get a "representation" of G.

Definition 155. Let G act on the set X. For $g \in G$, define $\sigma_g : X \to X$ by $a \longmapsto g \cdot a$. Then σ_g is a bijection, so $\sigma_g \in S(X) = \{\text{bijective maps } X \to X\}$. Then $\phi : G \to S(X)$ given by $g \longmapsto \sigma_g$ is a group homomorphism. When $|X| = n$, then $S(X) \cong S_n$. We say that ϕ is a *permutation representation* of G.

Example 156. 1. If $X = G$, we can consider the action of left multiplication or the action of conjugation.
2. If $X = G/H$, we can act by translation, i.e. $g \cdot aH = (ga)H$
3. If X is the set of Sylow $p-$subgroups of G, then we can act on X by conjugation.

Definition 157. Let k be a field, and V a $k-$vector space. We say G *acts $k-$linearly* if

1. G acts on V,
2. $g \cdot (\alpha v) = \alpha(g \cdot v)$ for all $v \in V$, $\alpha \in k$, $g \in G$, and
3. $g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2$ for all $g \in G$, $v_1, v_2 \in V$.

Remark 158. Given such a linear action, for each $g \in G$, we get a map ϕ_g in $\text{End}_R(V)^*$, the group of units of $\text{End}_R(V)$, defined by $\phi_g(v) = g \cdot v$ for all $v \in V$. This is in the group of units since $(\phi_g)^{-1} = \phi_{g^{-1}}$. Also, note that $GL_k(V) = \text{End}_R(V)$. So we get a group homomorphism $\rho : G \to GL_k(V)$ given by $g \longmapsto \phi_g$.

Definition 159. Let G be a group, and k a field. Then a *$k-$linear representation* of G is a homomorphism $\rho : G \to GL_k(V)$ for some $k-$vector space V.

Remark 160. Let $\rho : G \to GL_k(V)$ be a $k-$linear representation of G. This gives rise to a $k[G]-$module structure on V as follows. We already have that V is an abelian group under addition, so, given $v \in V$ and $\sum_{g \in G} a_g g \in k[G]$, we set $(\sum_{g \in G} a_g g)v = \sum_{g \in G} a_g \rho(g)(v) \in V$. Alternately, one could define $gv = \rho(g)(v)$ and extend the $G-$action by linearity. We'll denote V by V_ρ when we think of it as a $k[G]-$module.

3.8 Friday 9 March 2012

3.8.1 Representation Theory Vocab

Remark 161. If M is a $k[G]-$module, let ${}_kM$ be the underlying $k-$vector space. Then, given $g \in G$, the map $\phi_g :_k M \to_k M$ given by $m \longmapsto gm$ is an invertible $k-$endomorphism of ${}_kM$ and hence $\rho_M : G \to GL_k({}_kM)$ given by $g \longmapsto \phi_g$ is a group homomorphism.

Remark 162. We have constructed a bijection between $k-$linear representations of V and $k[G]-$modules.

Definition 163. Let G be a group, k a field, and $\rho : G \to GL_k(V)$ a $k-$linear representation of G.

1. A *subrepresentation* of ρ is a representation $\psi : G \to GL_k(W)$ where W is a subspace of V and for all $g \in G$, then $\rho(g)|_W = \psi(g)$.
2. The *zero representation* is the map $\rho : G \to GL_k(0)$. That is, as a $k[G]-$module, $0_\rho = 0$.
3. A representation, ρ, is called *irreducible* if it is not the zero representation and every subrepresentation is the zero representation or itself.
4. We define to representations $\rho_1 : G \to GL_k(V_1)$ and $\rho_2 : G \to GL_k(V_2)$ to be *isomorphic* if $(V_1)_{\rho_1} \cong (V_2)_{\rho_2}$ as $k[G]-$modules.
5. The *degree* of ρ is $\dim_k(V)$.
6. Given $\rho_i : G \to GL_k(V_i)$ for $i = 1, 2$, then we define $\rho_1 \oplus \rho_2 : G \to GL_k(V_1 \oplus V_2)$ by $g \longmapsto \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}$.
7. The representation $\rho : G \to k^* = GL_k(k) \cong M_1(k)$ given by $g \longmapsto 1_k$ is called the *trivial representation.*
8. Let $R = k[G]$. Then R is a left $k[G]-$module. Recall that $\rho_G : G \to GL_k({}_kR)$ is given by $g \longmapsto \phi_g$. We call this the *regular representation.*

Remark 164. Let G be a group, k a field, and $\rho : G \to GL_k(V)$ a $k-$linear representation of G.

1. If $\psi : G \to GL_k(W)$ is a subrepresentation of ρ, then we get that W_ψ is a $k[G]-$submodule of V_ρ.
2. The zero representation is a subrepresentation of every representation.
3. If ρ is an irreducible representation, then V_ρ is a simple $k[G]-$module.
4. If ρ_1 and ρ_2 are isomorphic, with $\phi : (V_1)_{\rho_1} \to (V_2)_{\rho_2}$ a $k[G]-$module isomorphism. Then ϕ is a $k-$linear isomorphism and $\phi(g \cdot v) = g \cdot \phi(v)$ for all $g \in G$ and $v \in V_1$. So, $(\phi \circ \rho_1(g))(v) = (\rho_2(g) \circ \phi)(v)$ for all $g \in G$ and $v \in V_1$. That is, $\rho_1(g) = \phi^{-1}\rho_2(g)\phi$ for all $g \in G$.
5. Degree 1 representations are irreducible.
6. The only degree 0 representation is the zero representation.
7. As $k[G]-$modules, $(V_1 \oplus V_2)_{\rho_1 \oplus \rho_2} \cong (V_1)_{\rho_1} \oplus (V_2)_{\rho_2}$.
8. The trivial representation has degree 1 and is hence irreducible.

3.8.2 Starting Examples of Representations

Example 165. Let $G = C_3 =< a \mid a^3 = 1 >$, and $R = k[G] = k \cdot 1 \oplus k \cdot a \oplus k \cdot a^2$. Then $\phi_a : R \to R$ is given by $1 \longmapsto a$, $a \longmapsto a^2$, and $a^2 \longmapsto 1$. Thus, we set $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \in GL_3(k)$. Then, we have that $A^3 = I_3$, the 3-by-3 identity matrix, and $\rho_R : C_3 \to GL_3(k)$ is given by $1 \longmapsto I_3$, $a \longmapsto A$ and $a^2 \longmapsto A^2$.[10]

Remark 166. Suppose that $k[G]$ is semisimple, which recall means that G is a finite group and that $\mathrm{char}(k) \nmid |G|$. Then every simple $k[G]-$module is isomorphic to a simple left ideal of $k[G]$, which is a direct summand of $k[G]$. Also, $k[G] \cong n_1 I_1 \oplus \ldots \oplus n_t I_t$ where I_j is simple for each j and every simple $k[G]-$module is isomorphic to some I_j. Thus, the regular representation $\rho_{k[G]} = n_1\rho_{I_1} \oplus \ldots \oplus n_t\rho_{I_t}$ where ρ_{I_j} is the irreducible subrepresentation corresponding to I_j for each j. Hence, every irreducible $k-$representation of G is a direct summand of the regular representation, and is isomorphic to ρ_{I_j} for some j.

Remark 167. The trivial representation is a subrepresentation of the regular representation for any group G. Indeed, set $R = k[G]$ and let $u = \sum_{g \in G} g$. Then $gu = u$ for all $g \in G$. Let $I = Ru = ku$. Then $\rho_I : G \to GL_k({}_kI)$ is given by $g \longmapsto 1$ and ρ_I is the trivial representation and a subrepresentation of the regular representation since I is a simple $k[G]-$module.

3.9 Monday 12 March 2012

3.9.1 Representations of Cyclic Groups and Permutation Groups

Example 168. Let $G = C_n =< a \mid a^n = 1 >$ and let k be an algebraically closed field of characteristic not dividing n. Every irreducible $k-$linear representation of G has degree 1, so there must be n such representations. Let $\rho : G \to GL_1(k) = k^*$ be given by $a \longmapsto \lambda \in k^*$. Since $a^n = 1$, then $\rho(a)^n = \lambda^n = 1$ so that λ must be an n^{th} root of unity.

[10] There are more details for this example in the handwritten notes.

Since the characteristic of the field does not divide n, then $x^n - 1$ has n distinct roots in k. In fact, the group of n^{th} roots of unity is cyclic, say generated by ω. then, $\rho_i : G \to GL_1(k)$ given by $a \longmapsto \omega^i$ gives all irreducible representations of G. From a module point of view, we set $R = k[C_n] = k \cdot 1 \oplus k \cdot a \oplus \ldots \oplus k \cdot a^{n-1}$ since $a^n = 1$. We then have

$$k[C_n] \cong k[x]/(x^n - 1) \cong k[x]/(x - \omega^0) \times \ldots \times k[x]/(x - \omega^{n-1}) = Re_0 \oplus \ldots \oplus Re_{n-1},$$

where $e_i = \overline{1}$ in $k[x]/(x - \omega^i)$. As $k-$vector spaces, $Re_i \cong k$ for each i so each Re_i is a simple left ideal. The action of G on Re_i is given by $a \cdot e_i = a \cdot \overline{1} = \overline{x} = \omega^i \cdot \overline{1} = \omega^i e_i$.

Remark 169. Suppose $H \lhd G$. Then any $k-$linear representation of G/H induces a $k-$linear representation for G. Indeed, if $\psi : G/H \to GL_k(V)$ is a $k-$representation for G/H then composition with the quotient map will give a $k-$representation for G:

$$\begin{array}{ccc} G & \xrightarrow{\rho} & GL_k(V) \\ & \searrow \quad \nearrow_{\psi} & \\ & G/H & \end{array}$$

Here, if ψ is an irreducible $k-$representation for G/H, then ρ is also an irreducible representation (for G).

Example 170. Let $G = S_n$, and $H = A_n$. Then for any n, we have $S_n/A_n \cong C_2 =< \sigma >$ for any $\sigma \in S_n \setminus A_n$. If k is a field of characteristic not equal to 2, then $\psi : C_2 \to k^*$ given by $\sigma \longmapsto -1$ is an irreducible, and nontrivial representation. Composing with the quotient map, we see that ρ is a nontrivial irreducible representation of S_n where $\rho : S_n \to k^*$ is given by $\sigma \longmapsto 1$ if $\sigma \in A_n$, and $\sigma \longmapsto -1$ if $\sigma \notin A_n$. That is, $\sigma \longmapsto \text{sgn}(\sigma) \cdot 1_k$. This representation is called the sign representation, and corresponds to the simple left ideal kw where $w = \sum_{\sigma \in S_n} \text{sgn}(\sigma)\sigma$.

Remark 171. Let $H \leq G$, and suppose $[G : H] = n$. Let $C_1, \ldots, C_n$ be the distinct left cosets of H in G. For each i, let $u_i = \sum_{g \in C_i} g \in k[G]$. Since for any $g \in G$, and any i, we have $gC_i = C_j$ for some j, then $gu_i = u_j$ for some j. Also, since the cosets are disjoint, then the set $\{u_1, \ldots, u_n\}$ is linearly independent over k. Let $I = ku_1 + \ldots + ku_n = ku_1 \oplus \ldots \oplus ku_n$. Since $gI \subseteq I$ for each $g \in G$, then I is a left ideal of $k[G]$. Note that I contains the left ideal $k(u_1 + \ldots + u_n) = k(\sum_{g \in G} g)$ so that I is not a simple left ideal unless $H = G$, that is, unless $n = 1$.

Example 172. Let $G = S_3$, and k be an algebraically closed field with $\text{char}(k) \nmid 6$ (that is, $\text{char}(k) \neq 2, 3$). Our goal is to find all irreducible $k-$representations of G. Since G has 3 conjugacy classes, there are 3 distinct irreducible $k-$representations. Let's call them ρ_1, ρ_2, and ρ_3 and set $n_i = \deg(\rho_i)$ for $i = 1, 2, 3$. Recall that $n_1^2 + n_2^2 + n_3^2 = 6$ so we must have that $n_1 = n_2 = 1$ and $n_3 = 2$. Let ρ_1 be the trivial representation, and ρ_2 be the sign representation. It remains then to find ρ_3. Note that if I_i is the ideal of $k[S_3]$ corresponding to ρ_i, then $k[S_3] = I_1 \oplus I_2 \oplus 2I_3$. Let's consider a left ideal corresponding to a subgroup H of S_3. If $|H| = 3$, then the corresponding ideal will have dimension 2. However, this ideal contains the trivial representation, and so decomposes into 2 simple ideals of dimension 1. So instead, we need to consider $H =< (12) >$. Let $C_1 = H$, $C_2 = (23)H$ and $C_3 = (13)H$, that is, as sets, $C_1 = \{(1), (12)\}$, $C_2 = \{(23), (132)\}$, and $C_3 = \{(13), (123)\}$. Let $u_i = \sum_{g \in C_i} g$, and let $I = ku_1 + ku_2 + ku_3$, which is a left ideal of $k[S_3]$ of dimension 3. Let $A = k(u_1 + u_2 + u_3) \subseteq I$. so $I = A \oplus J$, where $\dim_k(J) = 2$. If J is not simple, then $J = J_1 \oplus J_2$ where $\dim_k(J_i) = 1$ for $i = 1, 2$. But $k[S_3]$ contains only 2 simple left ideals of dimension 1. Thus, J must be a 2 dimensional simple left ideal, and correspond to the $k-$representation ρ_3. Consider the short exact sequence $0 \to A \to I \to I/A \to 0$. Since $I \cong A \oplus I/A$, then $J \cong I/A = \dfrac{ku_1 + ku_2 + ku_3}{k(u_1 + u_2 + u_3)} = k\overline{u_1} \oplus k\overline{u_2}$ and $\overline{u_3} = -\overline{u_1} - \overline{u_2}$. Thus, $\rho_3 : S_3 \to GL_2(k)$ is given by $(12) \longmapsto \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ and $(123) \longmapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. This is sufficient to define ρ_3 since these two elements generate S_3. Note that $(12)\overline{u_1} = \overline{u_1}$, $(12)\overline{u_2} = \overline{u_3} = -\overline{u_1} - \overline{u_2}$, $(123)\overline{u_1} = \overline{u_3} = -\overline{u_1} - \overline{u_2}$, and $(123)\overline{u_2} = \overline{u_1}$ which is how the representation ρ_3 was determined.

3.10 Wednesday 14 March 2012

3.10.1 Trace & Characters

Recall. If k is a field, and $A = [a_{ij}] \in M_n(k)$, then $\text{tr}(A) = \sum_{i=1}^n a_i i \in k$ is called the *trace* of A. Note that the map $\text{tr} : M_n(k) \to k$ is $k-$linear. Also, recall that $\text{tr}(AB) = \text{tr}(BA)$ for all $A, B \in M_n(k)$.
Now, if V is a finite dimensional $k-$vector space, and $\rho \in \text{End}_k(V)$, then $\text{tr}(\rho)$ is defined as $\text{tr}(\rho) = \text{tr}([\rho]_\beta)$ where $[\rho]_\beta$ is the matrix representation of ρ with respect to the basis β. Since $\text{tr}(PAP^{-1}) = \text{tr}(A)$, then $\text{tr}(\rho)$ is actually well defined, that is, it does not depend on the basis chosen.

Definition 173. Let k be a field, R a finite dimensional $k-$algebra, and let M be a finitely generated left $R-$module. For $r \in R$ define $r_M : M \to M$ by $a \longmapsto ra$. Then, $r_M \in \text{End}_R(M)$.

Note. If M is finitely generated over a finite dimensional $k-$algebra, R, then $\dim_k(M) < \infty$.

Definition 174. Define the *character* χ_M of the $R-$module M to be the map $\chi_M : R \to k$ given by $\chi_M(r) = \text{tr}(r_M)$.

Note. It is clear that χ_M is $k-$linear. Also, if $\{u_1, \ldots, u_n\}$ is a $k-$basis for R, then χ_M is uniquely determined by $\chi_M(u_1), \ldots, \chi_M(u_n)$.

Definition 175. The *degree* of χ_M is $\dim_k(M)$.

Remark 176. $\chi_M(1) = \text{tr}(id_M) = \dim_k(M) \cdot 1_k \in k$.

Remark 177. Let $\rho : G \to GL_k(V)$ be a $k-$representation of G, where G is a finite group. Then ρ corresponds to the $k[G]-$module V_ρ. The *character of* ρ is $\chi_{V_\rho} : k[G] \to k$. In this case, we often write χ_ρ to simplify notation, and consider $\chi_\rho : G \to k$ since G is a basis for $k[G]$, so χ_ρ is uniquely determined by $\chi_\rho(g)$ for $g \in G$. That is, $\chi_\rho(g) = \text{tr}(\rho(g))$. Also, we say that χ_ρ is a $k-$*character of* G.

Proposition 178. *Let R be a finite dimensional $k-$algebra, and $0 \to L \to M \to N \to 0$ a short exact sequence of left $R-$modules. Then, $\chi_M = \chi_L + \chi_N$.*

Proof. Let $r \in R$. We have a commutative diagram as below since for any $m \in M$, then $(r_N \circ g)(m) = rg(m) = g(rm) = (g \circ r_M)(m)$, and for any $\ell \in L$, then $(r_M \circ f)(\ell) = rf(\ell) = f(r\ell) = (f \circ r_L)(\ell)$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle r_L} & & \downarrow{\scriptstyle r_M} & & \downarrow{\scriptstyle r_N} & & \\ 0 & \longrightarrow & L & \xrightarrow[f]{} & M & \xrightarrow[g]{} & N & \longrightarrow & 0 \end{array}$$

As $k-$vector spaces, the rows are split exact. So we have that $M \cong L \oplus N$ as $k-$vector spaces. We then get

$$\chi_M(r) = \text{tr}(r_M) = \text{tr}(r_L \oplus r_N) = \text{tr}\begin{pmatrix} r_L & 0 \\ 0 & r_N \end{pmatrix} = \text{tr}(r_L) + \text{tr}(r_N) = \chi_L(r) + \chi_N(r)$$

since the following diagram commutes.[11]

$$\begin{array}{ccc} M & \cong & L \oplus N \\ \downarrow{\scriptstyle r_M} & & \downarrow{\scriptstyle r_L \oplus r_N} \\ M & \cong & L \oplus N \end{array}$$

□

Corollary 179. *Let R be a finite dimensional $k-$algebra.*

1. *If $N \subseteq M$ be finitely generated $R-$modules, then $\chi_M = \chi_N + \chi_{M/N}$.*
2. *If A and B are finitely generated $R-$modules, then $\chi_{A \oplus B} = \chi_A + \chi_B$.*
3. *If $M \cong N$, then $\chi_M = \chi_N$.*

Note. The converse of the third part of the corollary is false in general. An example is below.

Example 180. Let k be a field, and $R = k[x]/(x^2) = k \oplus k\overline{x}$. Also, let $M = R/(x) \oplus R/(x) \cong k \oplus k$. then, $xM = 0$, but $xR \neq 0$. So $M \ncong R$ even though $\dim_k(M) = \dim_k(R) = 2$.

A $k-$basis for R is $\{1, \overline{x}\}$. Also, $\chi_R(1) = \dim_k(R) \cdot 1_k = 2 \cdot 1_k$, and $\chi_R(\overline{x}) = \text{tr}\left(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right) = 0$. For M we have $\chi_M(1) = 2 \cdot 1_k$ and $\chi_M(\overline{x}) = \text{tr}\left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right) = 0$. Hence $\chi_R = \chi_M$.

Example 181. Let $R = k$, where k is a field of characterisitc 2. Also, let $M = R^2 = k^2$. Then $\chi_M(1) = \dim_k(M) = 2 \cdot 1_k = 0$. Thus, $\chi_M = 0$, but $M \ncong 0$.

[11] This was confusing this day, but is made clearer by an exercise and clarifiction near the beginning of Friday's class.

3.11 Friday 16 March 2012

3.11.1 Review/Clarification

Exercise. Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow[f]{} & B & \xrightarrow[g]{} & C & \longrightarrow & 0 \end{array}$$

be a commutative diagram of left $R-$modules such that the rows are split exact. then there exists an $R-$module isomorphism $\phi : B \to A \oplus C$ such that the following diagram commutes.

$$\begin{array}{ccc} B & \xrightarrow{\phi} & A \oplus C \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha \oplus \gamma} \\ B & \xrightarrow{\phi} & A \oplus C \end{array}$$

We've shown that there exist maps $i : B \to A$ and $j : C \to B$ such that $1_B = fi + jg$ and $if = 1_A$. This is shown by defining $\phi(b) = (i(b), g(b))$.

Note. In the proof of Proposition 178, the diagram below commutes due to the above exercise and ϕ is an isomorphism.

$$\begin{array}{ccc} M & \xrightarrow{\phi} & L \oplus N \\ \downarrow{\scriptstyle r_M} & & \downarrow{\scriptstyle r_L \oplus r_N} \\ M & \xleftarrow[\phi^{-1}]{} & L \oplus N \end{array}$$

Thus, $r_M = \phi \circ (r_L \oplus r_N) \circ \phi^{-1}$ and hence $\operatorname{tr}(r_B) = \operatorname{tr}(\phi \circ (r_L \oplus r_N) \circ \phi^{-1}) = \operatorname{tr}(r_L \oplus r_N)$.

3.11.2 Equality of Characters

Proposition 182. *Let R be a finite dimensional $k-$algebra, which is semisimple and $\operatorname{char}(k) = 0$. Also, let M and N be finitely generated $R-$modules. Then $M \cong N$ if and only if $\chi_M = \chi_N$.*

Proof. ($\Rightarrow$) This direction has been done, see Corollary 179.
($\Leftarrow$) Since R is semisimple, we can write $R \cong n_1 I_1 \oplus \ldots \oplus n_t I_t$ where each I_j is simple and $I_i \ncong I_j$ if $i \neq j$. We can also write $R \cong B(I_1) \oplus \ldots \oplus B(I_t)$ where $B(I_j) = \sum_{J \cong I_j} J$. We also have $M \cong m_1 I_1 \oplus \ldots \oplus m_t I_t$ and $N \cong r_1 I_1 \oplus \ldots \oplus r_t I_t$. It is enough to show that $m_i = r_i$ for all i. So we write, $M = N_1 \oplus \ldots \oplus N_t$ where $N_i \cong m_i I_i$ for each i, and let $e_i \in B(I_i) \subset R$ be the identity element of $B(I_i)$ for each i. We certainly have $e_i I_j = 0$ for all $i \neq j$ so $e_i N_j = 0$ for $i \neq j$. However, $e_i n = n$ for all $n \in N_i$. Consider the map

$$(e_i)_M = \begin{bmatrix} (e_i)_{N_1} & 0 & \cdots & 0 \\ 0 & (e_i)_{N_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & (e_i)_{N_t} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1_{N_i} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Thus, $\chi_M(e_i) = \operatorname{tr}(1_{N_i}) = \dim_k(N_i) \cdot 1_k = m_i \dim_k(I_i) \cdot 1_k$. Similarly, $\chi_N(e_i) = r_i \dim_k(I_i) \cdot 1_k$. Since $\chi_M = \chi_N$, then $m_i = r_i$ because $\operatorname{char}(k) = 0$. Thus, $M \cong N$. □

Corollary 183. *Let R be a semisimple, finite dimensional $k-$algebra, where k is a field of characteristic 0. If M is a finitely generated $R-$module, then $M = 0$ if and only if $\chi_M = 0$.*

Definition 184. A character $\chi_M \neq 0$ is said to be *irreducible* if whenever $\chi_M = \chi_N + \chi_{N'}$ for $R-$modules N, and N', then one of χ_N or $\chi_{N'}$ is 0.

Corollary 185. *Let R be a semisimple, finite dimensional $k-$algebra, where k is a field of characteristic 0. An $R-$module M is simple if and only if χ_M is irreducible.*

Corollary 186 (Recap). *Let R be a semisimple, finite dimensional $k-$algebra, where k is a field of characteristic 0. Then $R \cong n_1 I_1 \oplus \ldots \oplus n_t I_t$. Let M be a finitely generated $R-$module. Then $M \cong m_1 I_1 \oplus \ldots \oplus m_t I_t$. Denote χ_{I_i} by χ_i. Then,*

1. *χ_i is irreducible for all i,*
2. *$\chi_i \neq \chi_j$ for $i \neq j$,*
3. *$\{\chi_1, \ldots, \chi_t\}$ is the complete set of irreducible characters for R, and*
4. *$\chi_M = m_1\chi_1 + \ldots + m_t\chi_t$.*
5. *If additionally, we have that k is algebraically closed, then,*
   (a) *$n_i = \chi_i(1)$,*
   (b) *$\chi_R = \chi_1(1)\chi_1 + \ldots + \chi_t(1)\chi_t$, and*
   (c) *$\dim_k(R) = \chi_R(1) = \sum_{i=1}^t \chi_i(1)^2$.*

Recall. If $\rho : G \to GL_k(V)$ is a $k-$representation for G, then $\chi_\rho = \chi_{V_\rho}$ where V_ρ is the $k[G]-$module V (associated to ρ). If k has characterisitc 0 and G is a finite group, then the above apply to χ_ρ (although 5 only applies if k is algebraically closed). In this case, we usually consider $\chi_\rho : G \to k$ given by $g \longmapsto \mathrm{tr}(\rho(g))$, and call these $(k-)$characters of the group G.

Note. Let R be a semisimple, finite dimensional $k-$algebra, where k is a field of characteristic 0. Then χ_ρ is an irreducible character if and only if ρ is an irreducible representation.

3.11.3 Class Functions

Definition 187. A function $f : G \to A$ with G a group, and A a set, is called a *class function* if $f(gxg^{-1}) = f(x)$ for all $g, x \in G$. Equivalently, f is constant on conjugacy classes.

Remark 188. Group characters are class functions since we have

$$\chi_\rho(gxg^{-1}) = \mathrm{tr}(\rho(gxg^{-1})) = \mathrm{tr}(\rho(g)\rho(x)\rho(g)^{-1}) = \mathrm{tr}(\rho(x)) = \chi_\rho(x).$$

3.12 Monday 26 March 2012

3.12.1 Useful Character Theory Formulas

Recall. Our standard notation is as follows:

- ▷ G is a finite group, k is an algebraically closed field with $\mathrm{char}(k) \nmid |G|$
- ▷ Then, $k[G]$ is semisimple, and $k[G] = B(I_1) \times \ldots \times B(I_t) \cong n_1 I_1 \oplus \ldots \oplus n_t I_t$ where each I_j is simple, and $I_j \ncong I_i$ if $i \neq j$.
- ▷ We'll set $\chi_i = \chi_{I_i}$ for $i = 1, \ldots, t$, and $\phi = \chi_{k[G]}$, that is, ϕ is the character associated to the regular representation. Also, recall that $\phi = n_1\chi_1 + \ldots + n_t\chi_t$.
- ▷ Let e_i be the identity of $B(I_i)$.
- ▷ Let $C_1, \ldots, C_t$ be the distinct conjugacy classes of G and set $m_i = |C_i|$.
- ▷ Let $z_i = \sum_{g \in C_i} g \in k[G]$.
- ▷ Recall that $Z(k[G]) = ke_1 \times \ldots \times ke_t = kz_1 \oplus \ldots \oplus kz_t$.

Lemma 189. $\phi(g) = \begin{cases} |G|, & \text{if } g = 1 \\ 0, & \text{if } g \neq 1. \end{cases}$

Proof. Recall that $g_{k[G]} : k[G] \to k[G]$ is given by left multiplication by g, that is, $u \longmapsto gu$. Also, $\phi(g) = \mathrm{tr}(g_{k[G]})$. Thus, $\phi(1) = \mathrm{tr}(1_{k[G]}) = \dim_k(k[G]) = |G|$ since the matrix form of $1_{k[G]}$ is an $|G|$ by $|G|$ identity matrix. If $g \neq 1$, then $gh \neq h$ and since the elements of G form a basis for $k[G]$, then $g_{k[G]}$ permutes the basis elements and has no fixed points, so the matrix form of $g_{k[G]}$ has zeros on the main diagonal, and hence $\phi(g) = \mathrm{tr}(g_{k[G]}) = 0$. □

Theorem 190. *1. For $i = 1, \ldots, t$,*

$$e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

2. For any $g \in C_i$,

$$z_i = m_i \sum_{j=1}^{t} \frac{\chi_j(g)}{n_j} e_j.$$

Proof. 1. As $e_i \in k[G]$, we can write $e_i = \sum_{g\in G} a_g g$ where $a_g \in k$. Let $h \in G$, and consider $\phi(e_i h^{-1})$. By Lemma 189, and since characters are linear functions, we have

$$\phi(e_i h^{-1}) = \phi\left(\sum_{g\in G} a_g g h^{-1}\right) = \sum_{g\in G} a_g \phi(gh^{-1}) = a_h|G|.$$

On the other hand, we can compute the trace of $(e_i h^{-1})_{k[G]}$ to determine $\phi(e_i h^{-1})$. Since $e_i B(I_j) = 0$ for $i \neq j$, then $e_i h^{-1} B(I_j) = 0$ for $i \neq j$. Also, $e_i|_{B(I_j)}$ is the identity map on $B(I_j)$. The matrix form of $e_i h^{-1}_{k[G]}$ is therefore block diagonal, where the only nonzero diagonal block is for $B(I_i)$. Thus,

$$\operatorname{tr}((e_i h^{-1})_{k[G]}) = \operatorname{tr}((e_i h^{-1})_{B(I_i)}) = \operatorname{tr}(h^{-1}_{B(I_i)}) = n_i \chi_i(h^{-1})$$

since $B(I_j) \cong n_i I_i$ and $\chi_i(h^{-1}) = \operatorname{tr}(h^{-1}_{I_i})$. Putting this together, we have that $a_h|G| = n_i\chi_i(h^{-1})$. Hence,

$$a_h = \frac{n_i}{|G|}\chi_i(h^{-1})$$

for each $h \in G$, which gives the desired result.

2. By definition, $z_i = \sum_{g\in C_i} g$. Thus, for any $g \in C_i$ we have

$$\chi_j(z_i) = \chi_j\left(\sum_{g\in C_i} g\right) = \sum_{g\in C_i} \chi_j(g) = |C_i|\chi_j(g) = m_i\chi_j(g)$$

since χ_j is a class function. We can also write $z_i = \sum_{\ell=1}^{t} u_\ell e_\ell$ where $u_\ell \in k$. Thus,

$$\chi_j(z_i) = \chi_j\left(\sum_{\ell=1}^{t} u_\ell e_\ell\right) = \sum_{\ell=1}^{t} u_\ell \chi_j(e_\ell) = u_j\chi_j(1) = u_j n_j$$

since $\dim_k I_j = n_j$ and due to the linearity of χ_j. Putting this together, we have that $m_j\chi_j(g) = u_j n_j$ for any $g \in C_i$. Hence,

$$u_j = m_i\frac{\chi_j(g)}{n_j}$$

for any $g \in C_i$, which gives the desired result.

□

Note. Note that part 1 of Theorem 190 gives that $\operatorname{char}(k) \nmid n_i$ for all i.

Corollary 191. *1. For all $g \in G$ and $i, j \in \{1, \ldots, t\}$, then*

$$\sum_{g\in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}|G|$$

where $\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j. \end{cases}$

2. For all $g, h \in G$, then

$$\sum_{i=1}^{t} \chi_i(g)\chi_i(h^{-1}) = \Delta_{gh}|C_G(g)|$$

where $\Delta_{gh} = \begin{cases} 1, & \text{if } g \sim h \\ 0, & \text{if } g \nsim h \end{cases}$. *We use the notation $g \sim h$ to mean that g and h are conjugate, that is, there exists some $x \in G$ such that $xgx^{-1} = h$. Lastly, as usual, $C_G(g) = \{x \in G \mid gx = xg\}$ is the centralizer of g in G.*

3. If $g \neq 1$, then

$$\sum_{i=1}^{t} \chi_i(1)\chi_i(g) = 0.$$

Proof. 1. By Theorem 190, we know

$$e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

It is clear that $\chi_j(e_i) = 0$ whenever $i \neq j$. Also, when $i = j$, we have that $\chi_i(e_i) = \mathrm{tr}(1_{B(I_i)}) = n_i$. Thus, applying χ_j to the expression for e_i gives us that

$$\delta_{ij} n_i = \chi_j(e_i) = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})\chi_j(g).$$

Rearranging this gives the desired result.

2. By Theorem 190, we know that

$$z_i = m_i \sum_{j=1}^{t} \frac{\chi_j(g)}{n_j} e_j$$

for any fixed choice of $g \in C_i$. By definition, $z_i = \sum_{x \in C_i} x$. By plugging in the expression for e_i from Theorem 190 into the first expression for z_i we get

$$\begin{aligned} z_i &= m_i \sum_{j=1}^{t} \frac{\chi_j(g)}{n_j} \left(\frac{n_j}{|G|} \sum_{h \in G} \chi_j(h^{-1})h \right) \\ &= m_i \sum_{j=1}^{t} \sum_{h \in G} \frac{\chi_j(g) n_j}{n_j |G|} \chi_j(h^{-1})h \\ &= \frac{m_i}{|G|} \sum_{h \in G} \left(\sum_{j=1}^{t} \chi_j(g)\chi_j(h^{-1}) \right) h. \end{aligned}$$

Recall that by definition

$$z_i = \sum_{w \in C_i} w. \tag{3.1}$$

By comparing coefficients of the two expressions for z_i we obtain the following since the group elements are linearly independent. If $h \notin C_i$, then $\sum_{j=1}^{t} \chi_j(g)\chi_j(h^{-1}) = 0$ since h does not appear in the sum in equation (3.1). However, if $h \in C_i$, then we must have that $\frac{m_i}{|G|} \sum_{j=1}^{t} \chi_j(g)\chi_j(h^{-1}) = 1$. Since $|C_G(g)| = \frac{|G|}{m_i}$, then this establishes the desired formula.

3. If $g \neq 1$, then $g^{-1} \nsim 1$, and so we have by the previous part that

$$\sum_{i=1}^{t} \chi_i(1)\chi_i(g) = \Delta_{1g^{-1}} |C_G(1)| = 0.$$

□

3.13 Wednesday 28 March 2012

3.13.1 Character Tables

Remark 192. Each row of a character table corresponds to an irreducible character and each column corresponds to a conjugacy class in the group. The entry corresponding to the i^{th} character and j^{th} conjugacy class is $\chi_i(g)$ for some $g \in C_j$.

1. Since the number of irreducible characters equals the number of conjugacy classes, the tables are square.
2. Since characters are class functions, it does not matter which $g \in C_j$ is chosen.
3. The identity element of the group is always in its own conjugacy class, and $\chi_i(1)$ is always the degree of the representation (see Remark 176). This means that the first column of the table gets filled in with the degree of the given representation.
4. The character associated to the trivial representation is always at the top of the table, and the trivial representation sends every group element to 1 in the field, and hence every entry in the top row is a 1.
5. From part 3 of Corollary 191, we know that the dot product of the first column with any other column must be 0.

Example 193. Today we did lots of examples of character tables (and all were over the field $\mathbb{C}$.

1. Let $G = C_n =< a \mid a^n = 1 >$. Recall from Example 168 that the irreducible representations are $\{\rho_j \mid j = 0, \ldots, n-1\}$ where $\rho_j(a) = \omega^j$ and $\omega = e^{2\pi i/n}$. Let χ_j be the character associated to the representation ρ_j. In particular, if $n = 3$, then we have the following character table:

	1	a	a^2
χ_0	1	1	1
χ_1	1	ω	ω^2
χ_2	1	ω^2	ω

2. Let $G = V_4 = \{1, a, b, c\} \cong C_2 \times C_2$. The group is abelian, and so there are 4 conjugacy classes, and hence 4 irreducible representations all of degree 1. Let's call them ρ_0, ρ_1, ρ_2, and ρ_3. We know that ρ_j is determined by $\rho_j(a)$ and $\rho_j(b)$ since $ab = c$. We have then $\rho_j(a)^2 = \rho_j(b)^2 = \rho_j(1) = 1$ and so $\rho_j(a) = \pm 1$ and $\rho_j(b) = \pm 1$ for each j. There are 4 ways to choose between these, and so they must give our 4 irreducible representations. Let $\rho_0(a) = \rho_0(b) = 1$, $\rho_1(a) = -1$ and $\rho_1(b) = 1$, $\rho_2(a) = 1$ and $\rho_2(b) = -1$, and finally $\rho_3(a) = \rho_3(b) = -1$. Note that $\rho_j(c) = \rho_j(ab) = \rho_j(a)\rho_j(b)$. Since these are all elements of the field, then they are also the traces of the images of $\rho_j(g)$ for $g \in G$. This gives the following character table:

	1	a	b	c
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	1	-1	-1
χ_3	1	-1	-1	1

3. Let $G = S_3$. From Example 172, we know that there are 3 irreducible representations, and also where they send the group elements. Thus, we can quickly fill in the table, shown below. Alternately, using the fact that ρ_1 is the sign representation, we can get the first two rows, and fill in the third row using part 5 of Remark 192.

	(1)	(12)	(123)
χ_0	1	1	1
χ_1	1	-1	1
χ_2	2	0	-1

4. Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. The conjugacy classes of this group are $C_1 = \{1\}$, $C_2 = \{-1\}$, $C_3 = \{\pm i\}$, $C_4 = \{\pm j\}$, and $C_5 = \{\pm k\}$, so there must be 5 irreducible representations. We then have $8 = n_0^2 + n_1^2 + n_2^2 + n_3^2 + n_4^2$ and hence $n_0 = n_1 = n_2 = n_3 = 1$ and $n_4 = 2$. Let $H = \{\pm 1\}$ and note that $H \lhd G$. We also have that $G/H \cong C_2 \times C_2 \cong V_4$ since the elements of G/H are $\overline{1}$, $\overline{i}$, $\overline{j}$, $\overline{k}$ and $\overline{i}^2 = \overline{j}^2 = \overline{k}^2 = 1$. Since any irreducible representation of G/H gives an irreducible representation for G, by composing with the canonical map G/H this gives us that the degree 1 representations of G match the degree 1 representations of G/H, taking into account the fact that in G/H, C_1 and C_2 become the same conjugacy class. We can thus fill in all but the last row of the table using what we already know, and then get the bottom column using part 5 of Remark 192. The complete table is below:

	1	-1	i	j	k
χ_0	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	-1	1
χ_4	2	-2	0	0	0

5. Let $G = A_4$. The 4 conjugacy classes are $C_1 = \{(1)\}$, $C_2 = \{(12)(34), (13)(24), (14)(23)\}$, $C_3 = (123)H$ and $C_4 = (132)H$ where $H = C_1 \cup C_2$ is a normal subgroup of G. Thus there are 4 irreducible representations of A_4. Since $G/H \cong C_3$, there are at least 3 irreducible representations of degree 1. Since the sum of the squares of the degrees must equal the order of the group, i.e. we must have $n_0^2 + n_1^2 + n_2^2 + n_3^2 = 24$ then $n_0 = n_1 = n_2 = 1$ and $n_3 = 3$. In part 1 of this example, we found the character table for C_3, and we can fill in the remainder of the table using part 5 or Remark 192. The complete character table is below where $\omega = e^{2\pi i/3}$ as before.

	(1)	(12)(34)	(123)	(132)
χ_0	1	1	1	1
χ_1	1	1	ω	ω^2
χ_2	1	1	ω^2	ω
χ_3	3	-1	0	0

Remark 194. On the homework we show that if χ is a complex character (meaning that the field in question is the complex numbers) for a finite group G, then $\chi(g^{-1}) = \overline{\chi(g)}$. The first part of Corollary 191 gives

$$\sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{ij}|G|.$$

Now, let $g_1, \ldots, g_t$ be representatives of the conjugacy classes of G, and m_i be the number of elements in each conjugacy class. Then we have

$$\sum_{\ell=1}^{t} m_\ell \chi_i(g_\ell)\overline{\chi_j(g_\ell)} = \delta_{ij}|G|.$$

3.14 Friday 30 March 2012

3.14.1 Characters and Inner Products

Definition 195. Let G be a finite group, and k a field. Let $F_k(G)$ denote the set of class functions $G \to k$.

Note. It is clear that $F_k(G)$ is a $k-$vector space since $(f+g)(x) = f(x) + g(x)$ and $(cf)(x) = cf(x)$ for all $c \in k$, $x \in G$ and $f, g \in F_k(G)$. Also, $\dim_k F_k(G)$ is the number of conjugacy classes of G.

Definition 196. Let the inner product of $F_{\mathbb{C}}(G)$ be given by:

$$\langle \phi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}$$

and note that $\langle \phi, \psi \rangle \in \mathbb{C}$ for all $\phi, \psi \in F_{\mathbb{C}}(G)$.

Note. This is indeed an inner product. Here are the details:

▷ **Additive in the first variable:**

$$\begin{aligned} \langle \phi_1 + \phi_2, \psi \rangle &= \frac{1}{|G|} \sum_{g \in G} (\phi_1 + \phi_2)(g)\overline{\psi(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} (\phi_1(g) + \phi_2(g))\overline{\psi(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \phi_1(g)\overline{\psi(g)} + \frac{1}{|G|} \sum_{g \in G} \phi_2(g)\overline{\psi(g)} \\ &= \langle \phi_1, \psi \rangle + \langle \phi_2, \psi \rangle \end{aligned}$$

▷ **Compatiblity with scalars:**

$$\begin{aligned} \langle c\phi, \psi \rangle &= \frac{1}{|G|} \sum_{g \in G} (c\phi)(g)\overline{\psi(g)} \\ &= c\frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)} \\ &= c\langle \phi, \psi \rangle \end{aligned}$$

▷ **Conjugate Symmetry:**

$$\begin{aligned} \overline{\langle \phi, \psi \rangle} &= \overline{\frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}} \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)}\psi(g) \\ &= \langle \psi, \phi \rangle \end{aligned}$$

▷ **Positive Definiteness:**

$$\begin{aligned} \langle \phi, \phi \rangle &= \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\phi(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} |\phi(g)|^2 \geq 0 \end{aligned}$$

If $\phi = 0$, then it is clear that $\langle \phi, \phi, \rangle = 0$. If $\langle \phi, \phi \rangle = 0$, then $\sum_{g \in G} |\phi(g)|^2 = 0$. Since each $|\phi(g)|^2$ is a non-negative real number, then we must have that $|\phi(g)|^2 = 0$ for all $g \in G$ and hence $\phi(g) = 0$ for all $g \in G$.

Proposition 197. *The irreducible characters form an orthonormal basis for $F_{\mathbb{C}}(G)$. That is, if $\{\chi_1, \ldots, \chi_t\}$ are the irreducible characters, then $\langle \chi_i, \chi_j \rangle = \delta_{ij}$.*

Proof. Recall from Corollary 191 that $\sum_{g\in G}\chi_i(g)\chi_j(g^{-1}) = \delta_{ij}|G|$. Recall also from the homework that when the field is $\mathbb{C}$ we have $\chi_j(g^{-1}) = \overline{\chi_j(g)}$ for all irreducible characters χ_j. Thus, we can rearrange to obtain $|G|\delta_{ij} = \sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} = |G|\langle\chi_i,\chi_j\rangle$ which proves the proposition. □

Remark 198. We thus have that for all $\phi \in F_{\mathbb{C}}(G)$, that $\phi = \langle\phi,\chi_1\rangle + \ldots + \langle\phi,\chi_t\rangle\chi_t$.

Remark 199. Recall that ϕ is a character if and only if $\phi = m_1\chi_1 + \ldots + m_t\chi_t$ where $m_i \in \mathbb{N}_0$. Thus, $m_i = \langle\phi,\chi_i\rangle$. We then have that for any character ϕ, that $\langle\phi,\phi\rangle = m_1^2 + \ldots + m_t^2$.

Corollary 200. *A character ϕ is irreducible if and only if $\langle\phi,\phi\rangle = 1$.*

3.14.2 Localization

Remark 201. From now on, all rings are assumed to be commutative.

Definition 202. Let R be a commutative ring, and $S \subseteq R$ a multiplicatively closed set. Define a relation on $R \times S$ by $(r_1,s_1) \sim (r_2,s_2)$ when there exists some $t \in S$ such that $t(s_2r_1 - s_1r_2) = 0$ or equivalently when $ts_2r_1 = ts_1r_2$.

Proposition 203. *The relation in the previous definition is an equivalence relation.*

Proof. Let $r \in R$ and $s \in S$. Then for any $t \in S$, we have $tsr = tsr$ and so $(r,s) \sim (r,s)$. Also, if $(r_1,s_1) \sim (r_2,s_2)$, then there is some $t \in S$ such that $t(s_2r_1 - s_1r_2) = 0$. This also gives that $t(s_1r_2 - s_2r_1) = 0$ and so $(r_2,s_2) \sim (r_1,s_1)$. Finally, suppose that $(r_1,s_1) \sim (r_2,s_2)$ and $(r_2,s_2) \sim (r_3,s_3)$. Then there exist $t,t' \in S$ such that $ts_1r_2 = ts_2r_1$ and $t's_2r_3 = t's_3r_2$. Let $t'' = tt's_2$, and note that $t'' \in S$ since $t,t',s_2 \in S$ and S is multiplicatively closed. Then $t''s_3r_1 = tt's_2s_3r_1 = t'ts_2r_1s_3 = t'ts_1r_2s_3 = tt's_3r_2s_1 = tt's_2r_3s_1 = t''s_1r_3$ and so $(r_1,s_1) \sim (r_3,s_3)$. □

Definition 204. Let $\frac{r}{s}$ denote the equivalence class of (r,s). Then R_S is used to denote the set of equivalence classes, and is called the *localization of R at S*. Note here that $R_S = \left\{\frac{r}{s} \mid r \in R, s \in S\right\}$.

Theorem 205. *The localization of a commutative ring R at any multiplicatively closed set S is a commutative ring with identity under the following operations:*

$$\frac{r_1}{s_1}\cdot\frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2} \qquad \textit{and} \qquad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_2r_1 + s_1r_2}{s_1s_2}.$$

Proof. We need to show that these operations are well defined, and that they satisfy the ring axioms. First, assume that $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ and $\frac{r_3}{s_3} = \frac{r_4}{s_4}$. Then there exist t_1,t_2 such that $t_1s_2r_1 = t_1s_1r_2$ and $t_2s_4r_3 = t_2s_3r_4$. We need to show that $\frac{r_1r_3}{s_1s_3} = \frac{r_2r_4}{s_2s_4}$ and $\frac{s_3r_1 + s_1r_3}{s_1s_3} = \frac{s_4r_2 + s_2r_4}{s_2s_4}$. Let $t = t_1t_2$. Then we have

$$ts_2s_4r_1r_3 = t_1s_2r_1t_2s_4r_3 = t_1s_1r_2t_2s_3r_4 = ts_1s_3r_2r_4$$

so the first equality holds. We also have that

$$\begin{aligned} ts_2s_4(s_3r_1 + s_1r_3) &= (t_1s_2r_1)t_2s_4s_3 + (t_2s_4r_3)t_1s_2s_1 \\ &= (t_1s_1r_2)t_2s_4s_3 + (t_2s_3r_4)t_1s_2s_1 \\ &= t_1t_2s_1s_3s_4r_2 + t_1t_2s_1s_3s_2r_4 \\ &= ts_1s_3(s_4r_2 + s_2r_4) \end{aligned}$$

so that the second equality holds and hence the operations are well defined. Note next that $\frac{r_1r_2}{s_1s_2}$ and $\frac{s_2r_1 + s_1r_2}{s_1s_2}$ are elements of R_S for any $r_1,r_2 \in R$ and any $s_1,s_2 \in S$ since S is multiplicatively closed and hence R_S is closed under both addition and multiplication. Also, if $r \in R$ and $s,s' \in S$, then $\frac{r}{s} + \frac{0}{s'} = \frac{s'r + s0}{ss'} = \frac{s'r}{ss'} = \frac{r}{s}$ since for any $t \in S$, we have $ts(s'r) = t(ss')r$. Thus, $\frac{0}{s'}$ is the additive identity. Also, if $r \in R$ and $s \in S$, then $-r \in R$ and we have $\frac{r}{s} + \frac{-r}{s} = \frac{sr - sr}{ss} = \frac{0}{ss} = \frac{-sr + sr}{ss} = \frac{-r}{s} + \frac{r}{s}$ and so $\frac{-r}{s}$ is the additive inverse of $\frac{r}{s}$. Next, for any $r,r' \in R$ and

$s, s' \in S$, we have $\frac{r}{s} + \frac{r'}{s'} = \frac{s'r + sr'}{ss'} = \frac{sr' + s'r}{s's} = \frac{r'}{s'} + \frac{r}{s}$. In order to show addition is associative, let $r, r', r'' \in R$ and $s, s', s'' \in S$. Then using that R is a ring, we have

$$\begin{aligned}
\left(\frac{r}{s} + \frac{r'}{s'}\right) + \frac{r''}{s''} &= \frac{s'r + sr'}{ss'} + \frac{r''}{s''} \\
&= \frac{s''(s'r + sr') + ss'r''}{ss's''} \\
&= \frac{s's''r + ss''r' + ss'r''}{ss's''} \\
&= \frac{s's''r + s(s''r' + s'r'')}{ss's''} \\
&= \frac{r}{s} + \frac{s''r' + s'r''}{s's''} \\
&= \frac{r}{s} + \left(\frac{r'}{s'} + \frac{r''}{s''}\right)
\end{aligned}$$

and hence $(R_S, +)$ is an abelian group as desired. To see that multiplication is associative, let $r, r', r'' \in R$ and $s, s', s'' \in S$. Then, $\left(\frac{r}{s} \cdot \frac{r'}{s'}\right) \cdot \frac{r''}{s''} = \frac{rr'}{ss'} \cdot \frac{r''}{s''} = \frac{rr'r''}{ss's''} = \frac{r}{s} \cdot \frac{r'r''}{s's''} = \frac{r}{s} \cdot \left(\frac{r'}{s'} \cdot \frac{r''}{s''}\right)$ using only the associativity of R. Next, let $s, s' \in S$ and $r \in R$. Then for any $t \in S$, we have $ts(rs') = t(ss')r$ and hence $\frac{r}{s} \cdot \frac{s'}{s'} = \frac{rs'}{ss'} = \frac{r}{s} = \frac{s'r}{s's} = \frac{s'}{s'} \cdot \frac{r}{s}$ so that $\frac{t}{t}$ is the multiplicative identity of R_S. For any $r, r' \in R$ and any $s, s' \in S$, we have $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'} = \frac{r'r}{s's} = \frac{r'}{s'} \cdot rs$ so that multiplication is commutative. It only remains to show then that multiplication distributes over addition. So let $r, r', r'' \in R$ and $s, s', s'' \in S$. Then,

$$\begin{aligned}
\left(\frac{r}{s} + \frac{r'}{s'}\right) \cdot \frac{r''}{s''} &= \frac{s'r + sr'}{ss'} \cdot \frac{r''}{s''} \\
&= \frac{(s'r + sr')r''}{ss's''} \\
&= \frac{s'rr'' + sr'r''}{ss's''} \\
&= \frac{s's''rr'' + ss''r'r''}{ss''s's''} \\
&= \frac{rr''}{ss''} + \frac{r'r''}{s's''} \\
&= \frac{r}{s} \cdot \frac{r''}{s''} + \frac{r'}{s'} \cdot \frac{r''}{s''}.
\end{aligned}$$

This completes the proof that R_S is a commutative ring with identity under the given operations. □

Remark 206. The following are easy, but it is worth going through the proofs once.[12]

▷ The ring $R_S = \{0\}$ if and only if $0 \in S$.

Proof. If $0 \in S$, then $\frac{r}{s} = \frac{0}{t}$ for any $s, t \in S$ and $r \in R$ since $0tr = 0s0$. Conversely, if $R_S = \{0\}$, then $\frac{1}{s} = \frac{0}{s}$ for any $s \in S$ and so there is some $t \in S$ such that $ts1 = ts0$ so that $ts = 0$. Since S is multiplicatively closed, this gives that $0 = ts \in S$. □

▷ Let $S' = S \cup \{1\}$. Then $R_S \cong R_{S'}$ and so without loss of generality, we usually assume $1 \in S$.

Proof. Let $\phi : R_S \to R_{S'}$ be given by $\frac{r}{s} \longmapsto \frac{r}{s}$. This map is well defined since if $\frac{r}{s} = \frac{r'}{s'}$ in R_S, then there is some $t \in S$ such that $tsr' = ts'r$ and since $t \in S'$, then $\frac{r}{s} = \frac{r'}{s'}$ in $R_{S'}$ as well. Next, we'll show that it is a ring

[12] I hope! Definitely not worth going through them more than once!!!

homomorphism. Let $r_1, r_2 \in R$ and $s_1, s_2 \in S$. Then,

$$\phi\left(\frac{r_1}{s_1} \cdot \frac{r_2}{s_2}\right) = \phi\left(\frac{r_1 r_2}{s_1 s_2}\right) = \frac{r_1 r_2}{s_1 s_2} = \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \phi\left(\frac{r_1}{s_1}\right) \cdot \phi\left(\frac{r_2}{s_2}\right)$$

and similarly

$$\phi\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) = \phi\left(\frac{s_2 r_1 + s_1 r_s}{s_1 s_2}\right) = \frac{s_2 r_1 + s_1 r_s}{s_1 s_2} = \frac{r_1}{s_1} + \frac{r_2}{s_2} = \phi\left(\frac{r_1}{s_1}\right) + \phi\left(\frac{r_2}{s_2}\right).$$

Now, if $\phi\left(\frac{r}{s}\right) = 0$, then there exists some $t \in S'$ such that $tr = 0$. If $t = 1$, then $r = 0$ and $\frac{r}{s} = 0$. If $t \neq 1$, then $t \in S$, and so $\frac{r}{s} = 0$ in R_S. Hence, ϕ is injective. If $\frac{r}{s} \in R_{S'}$ and $s \in S$, then $\phi\left(\frac{r}{s}\right) = \frac{r}{s}$. If $\frac{r}{s} \in R_{S'}$ and $s = 1$, then for any $s' \in S$, we have $\frac{rs'}{ss'} = \frac{r}{s}$ and so $\phi\left(\frac{rs'}{ss'}\right) = \frac{r}{s}$ so that ϕ is surjective and hence an isomorphism.. □

▷ There is a natural ring homomorphism $\phi : R \to R_S$ given by $r \longmapsto \frac{r}{1}$.

Proof. We only need to show that this is indeed a ring homomorphism. So let $r, r' \in R$. Then $\phi(rr') = \frac{rr'}{1} = \frac{r}{1} \cdot \frac{r'}{1} = \phi(r)\phi(r')$. Similarly, $\phi(r + r') = \frac{r + r'}{1} = \frac{r}{1} + \frac{r'}{1} = \phi(r) + \phi(r')$. Thus, ϕ is a ring homomorphism. □

▷ The map ϕ in the previous remark is injective if and only if S does not contain any zero divisors.

Proof. ($\Rightarrow$) Suppose that $t \in S$ such that $ta = 0$ for some $a \in R$. Then $\phi(ta) = 0$, meaning that $\frac{ta}{1} = \frac{t}{1} \cdot \frac{a}{1} = \frac{0}{1}$ in R_S. Since $t \in S$, then we multiply by $\frac{1}{t}$ to get $\frac{0}{1} = \frac{1}{t} \cdot \frac{t}{1} \cdot \frac{a}{1} = \frac{a}{1} = \phi(a)$. Since we're assuming that ϕ is injective, this means that $a = 0$ so that t is not a zero divisor.
($\Leftarrow$) Suppose that $\phi(a) = 0$. Then $\frac{a}{1} = \frac{0}{1}$ and so there is some $t \in S$ such that $t(a - 0) = 0$ or equivalently that $ta = 0$. Since S doesn't include any zerodivisors, this then means that $a = 0$. □

▷ $\phi(t)$ is a unit for all $t \in S$.

Proof. Since $t \in S$, then $\frac{1}{t} \in R_S$. Also, $\frac{1}{t} \cdot \phi(t) = \frac{1}{t} \cdot \frac{t}{1} = \frac{t}{t}$ which is the identity element of R_S. □

Note. Sometimes, and especially in older literature, the notation $S^{-1}R$ is used instead of R_S.

Example 207. These examples don't require proofs.[13]

▷ If R is a domain, and $S = R \setminus \{0\}$, then $R_S = Q(R)$ is the field of fractions of R.
▷ More generally, if R is an arbitrary commutative ring, and S is the set of non-zerodivisors of R, then S is multiplicatively closed and R_S is called the *total quotient ring* of R.
▷ If S consists of only units, then $R_S \cong R$.
▷ If $x \in R$, then $S = \{x^n \mid n \in \mathbb{N}_0\}$ is multiplicatively closed. We usually denote R_S by R_x in this case. Note here that $R_x = \left\{\frac{r}{x^n} \mid r \in R, n \in \mathbb{N}_0\right\}$.
▷ We thus have $\mathbb{Z}_2 = \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\right\} = \mathbb{Z}\left[\frac{1}{2}\right]$.
▷ Let $R = k[x]$ where x is an indeterminate and k is a field. Then $R_x = k[x, x^{-1}]$.

Remark 208. If $ab = 0$ in R but $a, b \neq 0$, and we want to make a into a unit, i.e. so that $\phi^{-1}(a)$ exists, then we must set $\phi(b) = 0$ since $0 = \phi(ab) = \phi(a)\phi(b)$.

[13] At least not at this point in my opinion.

3.15 Monday 2 April 2012

3.15.1 Facts about Localization

Remark 209. Let $P \in \text{Spec}(R)$. Then $S = R \setminus P$ is a multiplicatively closed set. Instead of writing R_S, in this case the notation R_P is used.[14]

Proposition 210. *Let I be an ideal of R. Then, $I_S = \left\{ \frac{r}{s} \mid r \in I, s \in S \right\}$ is an ideal of R_S. Note however that we can have $\frac{r}{s} = \frac{r'}{s'}$ with $r' \notin I$, but $r \in I$.*

Proof. Let $\frac{a}{s}, \frac{a'}{s'} \in I_S$, with $a, a' \in I$. Then, $\frac{a}{s} - \frac{a'}{s'} = \frac{s'a - sa'}{ss'} \in I_S$ since $s'a, -sa' \in I$, and hence $s'a - sa' \in I$ due to I being an ideal. Also, if $\frac{r}{s''} \in R_S$, then $\frac{r}{s''}\frac{a}{s} = \frac{ra}{s''s} \in I_S$ since $ra \in I$ due to I being an ideal. Thus, I_S is an ideal of R_S for every ideal I of R. □

Proposition 211. *In fact, every ideal of R_S is of the form I_S where I is an ideal of R.*

Proof. Let J be an ideal of R_S and set $I = \phi^{-1}(J)$ where $\phi : R \to R_S$ is the ring homomorphism given by $r \longmapsto \frac{r}{1}$. Then, I is an ideal since ϕ is a ring homomorphism. It remains to show that $I_S = J$. First, let $\frac{a}{s} \in I_S$ where $a \in I$ and $s \in S$. Then $\phi(a) = \frac{a}{1} \in J$ by definition of I and so $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} \in J$ since J is an ideal. Next, let $\frac{a}{s} \in J$. Then since J is an ideal, we have $\frac{a}{1} = \frac{a}{s} \cdot \frac{s}{1} \in J$. Thus, $a \in \phi^{-1}(J) = I$. □

Proposition 212. *If I is an ideal of R, generated by $a_1, \ldots, a_n$, then I_S is an ideal of R_S generated by $\frac{a_1}{1}, \ldots, \frac{a_n}{1}$. In particular, if R is Noetherian, then R_S is also Noetherian.*

Proof. Since I is generated by $a_1, \ldots, a_n$, then every element of I looks like $r_1a_1 + \ldots + r_na_n$ where $r_i \in R$ for all i. Thus, if $\frac{x}{s} \in I_S$, then $\frac{x}{s} = \frac{a}{s}$ where $a \in I$. We then have that $a = r_1a_1 + \ldots + r_na_n$ for some $r_i \in R$ and hence, $\frac{x}{s} = \frac{a}{s} = \frac{r_1a_1}{s} + \ldots + \frac{r_na_n}{s} = \frac{r_1}{s}\frac{a_1}{1} + \ldots + \frac{r_n}{s}\frac{a_n}{1}$ so that I_S is now seen to be generated by $\frac{a_1}{1}, \ldots, \frac{a_n}{1}$. □

Proposition 213. *Let R be a commutative ring and S a multiplicatively closed subset of R. Then, $I_S = R_S$ if and only if $I \cap S \neq \emptyset$.*

Proof. ($\Rightarrow$) If $\frac{1}{1} \in I_S$, then $\frac{1}{1} = \frac{a}{s}$ for some $a \in I$ and $s \in S$. Thus, there exists a $t \in S$ such that $ts = ta \in S \cap I$ since $ts \in S$ and $ta \in I$ are clear since S is multiplicatively closed and $a \in I$ with I an ideal.

($\Leftarrow$) Suppose that $I \cap S \neq \emptyset$. Then there is some $a \in I \cap S$. Then, $\frac{1}{1} = \frac{a}{a} \in I_S$ since $a \in I$ and $a \in S$ and so $I_S = R_S$. □

Remark 214. If $J \subseteq I$ are ideals of R and S is a multiplicatively closed subset of R, then $J_S \subseteq I_S$.

Example 215. Let $R = \mathbb{Z}$, and $S = \{2^n \mid n \in \mathbb{N}_0\}$. Then note that $(6) \subsetneq (3)$ as ideals in $\mathbb{Z}$, but in R_S, we have that $(3)_S = (6)_S$ since $\frac{3}{1} = \frac{1}{2} \cdot \frac{6}{1} \in (6)_S$.

Proposition 216. *Let R be a commutative ring, S a multiplicatively closed subset of R, and $\phi : R \to R_S$ the ring homomorphism given by $r \longmapsto \frac{r}{1}$. Then there is a bijection*

$$\{P \in \text{Spec}(R) \mid P \cap S = \emptyset\} \longleftrightarrow \{P \in \text{Spec}(R_S)\}$$

given by $P \longmapsto P_S$ and $\phi^{-1}(Q) \longleftarrow\!\shortmid Q$.

Proof. First, let $P \in \{P \in \text{Spec}(R) \mid P \cap S = \emptyset\}$. We need to show that $P_S \in \text{Spec}(R_S)$. We already know that P_S is an ideal of R_S and we know that $P_S \subsetneq R_S$ by Proposition 213 since $P \cap S = \emptyset$. Thus, let $\frac{a}{s} \cdot \frac{b}{s'} \in P_S$. Then $\frac{a}{s} \cdot \frac{b}{s'} = \frac{p}{s''}$ where $p \in P$ and $s'' \in S$. Then there exists some $t \in S$ such that $ts''ab = tss'p$. Note then that $ts''ab \in P$ since P

[14] Although this is a special case of localization, it is the one used most frequently.

is an ideal. Since $ts'' \in S$, then $ts'' \notin P$ and so we must have $ab \in P$. Since P is prime, then $a \in P$ or $b \in P$ and hence one of $\frac{a}{s}$ or $\frac{b}{s'}$ is in P_S.

Next, it is clear that $\phi^{-1}(Q) \in \text{Spec}(R)$ for all $Q \in \text{Spec}(R_S)$ since pre-images of prime ideals are prime. Also, if $Q \in \text{Spec}(R_S)$, then $Q \neq R_S$. Consider $\phi^{-1}(Q) \cap S$. If $a \in \phi^{-1}(Q) \cap S$, then $\phi(a) = \frac{a}{1} \in Q$ and $\frac{1}{a} \in R_S$ and so $\frac{a}{a} \in Q$ so that $Q = R_S$. This would be a contradiction, and so we must have that $\phi^{-1}(Q) \cap S = \emptyset$ and hence $\phi^{-1}(Q) \in \{P \in \text{Spec}(R) \mid P \cap S = \emptyset\}$.

Next, we need to show $\phi^{-1}(Q)_S = Q$. If $\frac{a}{s} \in Q$, then $a \in \phi^{-1}(Q)$ and so $\frac{a}{s} \in \phi^{-1}(Q)_S$ and hence $Q \subseteq \phi^{-1}(Q)_S$. On the other hand, if $\frac{a}{s} \in \phi^{-1}(Q)_S$, then we have $\frac{a}{s} = \frac{b}{s'}$ where $b \in \phi^{-1}(Q)$ and $s' \in S$. Then, $\frac{b}{1} \in Q$ and since Q is an ideal and $\frac{1}{s'} \in R_S$, we then have $\frac{a}{s} = \frac{b}{s'} = \frac{b}{1} \cdot \frac{1}{s'} \in Q$ and hence $\phi^{-1}(Q) = Q$.

Finally, we need to show that $\phi^{-1}(P_S) = P$. If $a \in \phi^{-1}(P_S)$, then $\frac{a}{1} \in P_S$ so that $\frac{a}{1} = \frac{b}{s}$ for some $b \in P$ and $s \in S$. Thus, there exists some $t \in S$ such that $tsa = tb$. This element is in P since $b \in P$. Thus, since $s, t \in S$ and hence $s, t \notin P$, we have $a \in P$. This shows that $\phi^{-1}(P_S) \subseteq P$. For the reverse direction, if $a \in P$, then $\frac{a}{1} \in P_S$ and so $a \in \phi^{-1}(P_S)$ is clear. □

Example 217. Let $R = \mathbb{Z}$ and $S = \{2^n \mid n \in \mathbb{N}_0\}$. We have $\text{Spec}(\mathbb{Z}) = \{(p) \mid p \text{ prime}\} \cup \{0\}$ and $\text{Spec}(R_S) = \text{Spec}(\mathbb{Z}_2) = \{(p)_s \mid p \text{ an odd prime}\} \cup \{(0)_2\}$.

Example 218. If $R = \mathbb{Z}$ and $S = R \setminus (2)$, then $\mathbb{Z}_{(2)} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \notin 2\mathbb{Z}\right\}$. Also, $\text{Spec}(R_S) = \text{Spec}(\mathbb{Z}_{(2)} = \{(0)_{(2)}, (2)_{(2)}\}$.

Definition 219. A commutative ring R is said to be *quasi-local* if R has a unique maximal ideal. A commutative ring R is said to be *local* if it is quasi-local and Noetherian. If R is a quasi-local ring, with maximal ideal $\mathfrak{m}$, then the *residue field* of R is $R/\mathfrak{m}$.

Remark 220. If R is a ring, and $P \in \text{Spec}(R)$, then R_P is a quasi-local ring with maximal ideal $P_P = PR_P$.

Proof. Indeed, if $Q \in \text{Spec}(R_P)$, then $Q = q_P$ for some $q \in \text{Spec}(R)$ and $q \cap (R \setminus P) = \emptyset$. Thus, $q \subseteq P$ and so $Q = q_P \subseteq P_P$. □

3.16 Wednesday 4 April 2012

3.16.1 Localization of Modules

Definition 221. Let M be an $R-$medule, and S a multiplicatively closed subset of R. For $m \in M$ and $s \in S$, let $\frac{m}{s}$ denote the equivalence class of $(m, s) \in M \times S$ where the equivalence relation is given by $(m, s) \sim (m', s')$ if and only if there is some $t \in S$ such that $t(s_2 m_1 - s_1 m_2) = 0$. Also, set $M_S = \left\{\frac{m}{s} \mid m \in M, s \in S\right\}$. This is called the *localization of M at S*.

Theorem 222. *The localization of M at S is an R_S-module under the following operations:*

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \qquad \text{and} \qquad \frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'}$$

Proof. The proof is very similar to the proof of Theorem 205.[15] □

Remark 223. These remarks are easy, and the proofs are similar to the similar cases for rings, so the proofs will be omitted.

- ▷ There is a natural $R-$module homomorphism $\alpha : M \to M_S$ given by $m \longmapsto \frac{m}{1}$.
- ▷ Given an $R-$submodule N of M, then N_S is an R_S-submodule of M_S.
- ▷ If T is an R_S-submodule of M_S, then $T = N_S$ where $T = \alpha^{-1}(T)$.
- ▷ If $N = Rx_1 + \ldots + Rx_n$, then $N_S = R_S\frac{x_1}{1} + \ldots + R_S\frac{x_n}{1}$.

Note. The $R-$submodules of M_S are potentially different than the R_S-submodules of M_S. For example, $\mathbb{Z}_{(0)} = \mathbb{Q}$. The $\mathbb{Z}-$submodules of a module may be different than the $\mathbb{Q}-$submodules of the same module.

Proposition 224. *If M is a Noetherian (resp. Artinian) module over a ring R, and S is a multiplicatively closed subset of R, then M_S is a Noetherian (resp. Artinian) R_S-module.*

[15] And is no longer worth doing for me.

Proof. The Noetherian case is super similar to the Artinian case.[16] Suppose $T_0 \supseteq T_1 \supseteq \dots$ is a decreasing chain of R_S-submodules of M_S. Then, $\alpha^{-1}(T_0) \supseteq \alpha^{-1}(T_1) \supseteq \dots$ is a descending chain of $R-$submodules of M. Since M is Artinian, then there exists some $k \in \mathbb{N}_0$ such that $\alpha^{-1}(T_k) = \alpha^{-1}(T_{k+i})$ for all $i \in \mathbb{N}_1$. This means that $(\alpha^{-1}(T_k))_S = (\alpha^{-1}(T_{k+i}))_S$ for all $i \in \mathbb{N}_1$. However taking the inverse image and then localizing gives the module you started with, and so $T_k = T_{k+i}$ for all $i \in \mathbb{N}_1$. □

Proposition 225. *Let M be an $R-$module. The following are equivalent:*

1. $M = 0$,
2. $M_P = 0$ *for all* $P \in \operatorname{Spec} R$, *and*
3. $M_{\mathfrak{m}} = 0$ *for all maximimal ideals* $\mathfrak{m}$.

Proof. $(1 \Rightarrow 2)$ If $M = 0$, then it is clear that any localization of M is also zero, and in particular, $M_P = 0$ for all prime ideals P.

$(2 \Rightarrow 3)$ If $M_P = 0$ for every prime ideal P, then if $\mathfrak{m}$ is a maximal ideal, it is also a prime ideal, and hence $M_{\mathfrak{m}} = 0$.

$(3 \Rightarrow 1)$ Let $x \in M$, and let $I = \operatorname{Ann}_R(x) = \{r \in R \mid rx = 0\}$. Then I is an ideal of R since R is a commutative ring. Note that $x = 0$ if and only if $I = R$, which is true if and only if $I \subsetneq \mathfrak{m}$ for any maximal ideal $\mathfrak{m}$. Let $\mathfrak{m}$ be a maximal ideal. Since $M_{\mathfrak{m}} = 0$, then $\dfrac{x}{1} = \dfrac{0}{1}$ in $M_{\mathfrak{m}}$. Thus, there is some $t \in R \setminus \mathfrak{m}$ such that $tx = t(1x - 10) = 0$. Thus, $t \in \operatorname{Ann}_R(x) = I$. Hence $I \not\subset \mathfrak{m}$ and so $I = R$ and $x = 0$. □

Example 226. Let F be a field, and $R = F \times F$. Then $\operatorname{Spec}(R) = \{F \times (0), (0) \times F\} = \{\mathfrak{m}_1, \mathfrak{m}_2\}$. Then $R_{\mathfrak{m}_i} \cong F$ for $i = 1, 2$, which is a field, but R is not a domain.

Lemma 227. *Let $\{M_i\}_{i \in I}$ be a collection of $R-$modules, and S a multiplicatively closed subset of R. Then*

$$\left(\bigoplus_{i \in I} M_i\right)_S \cong \bigoplus_{i \in I} (M_i)_S$$

where the map is given by $\dfrac{(m_i)}{s} \longmapsto \left(\dfrac{m_i}{s}\right)$.

Proof. We first need to show that this map is well defined. So suppose that $\dfrac{(m_i)}{s} = \dfrac{(m_i')}{s'}$ in $\left(\bigoplus_{i \in I} M_i\right)_S$. Then there exists some $t \in S$ such that $ts'(m_i) = ts(m_i')$. Hence, for all $i \in I$, we have $ts'm_i = tsm_i'$. Thus, for all $i \in I$, $\dfrac{m_i}{s} = \dfrac{m_i'}{s'}$ in $(M_i)_S$. Therefore, $\left(\dfrac{m_i}{s}\right) = \left(\dfrac{m_i'}{s'}\right)$. Next, we'll show that this is a homomorphism of R_S-modules. Let $\dfrac{(m_i)}{s}, \dfrac{(m_i')}{s'} \in \left(\bigoplus_{i \in I} M_i\right)_S$. Then,

$$\phi\left(\frac{(m_i)}{s} + \frac{(m_i')}{s'}\right) = \phi\left(\frac{(s'm_i + sm_i')}{ss'}\right) = \left(\frac{s'm_i + sm_i'}{ss'}\right) = \left(\frac{m_i}{s} + \frac{m_i'}{s'}\right) = \left(\frac{m_i}{s}\right) + \left(\frac{m_i'}{s'}\right) = \phi\left(\frac{(m_i)}{s}\right) + \phi\left(\frac{(m_i')}{s'}\right)$$

and if $\frac{r}{s'} \in R_S$, then

$$\phi\left(\frac{r}{s'} \cdot \frac{(m_i)}{s}\right) = \phi\left(\frac{(rm_i)}{s's}\right) = \left(\frac{rm_i}{s's}\right) = \frac{r}{s'}\left(\frac{m_i}{s}\right) = \frac{r}{s}\phi\left(\frac{(m_i)}{s}\right)$$

so that ϕ is an R_S-module homomorphism. It only then remains to show that the map is bijective. So, suppose that $\phi\left(\dfrac{(m_i)}{s}\right) = \phi\left(\dfrac{(m_i')}{s'}\right)$. Then $\left(\frac{m_i}{s}\right) = \left(\frac{m_i'}{s'}\right)$ and hence there exists a finite set $\Gamma \subset I$ such that $m_i = n_i = 0$ for all $i \in I \setminus \Gamma$. However, for each $i \in \Gamma$, we have that there exists some $t_i \in S$ such that $t_i s'm_i = t_i sm_i'$. Let $t = \prod_{i \in \Gamma} t_i$ and notice that $t \in S$ since S is multiplicatively closed. Then, we have that $ts'(m_i) = ts(m_i')$ since $ts'm_i = tsm_i'$ for all $i \in \Gamma$ and $ts'm_i = tsm_i' = 0$ for all $i \notin \Gamma$. Thus, $\dfrac{(m_i)}{s} = \dfrac{(m_i')}{s'}$ and ϕ is injective. Finally, let $\left(\dfrac{m_i}{s_i}\right) \in \bigoplus_{i \in I} (M_i)_S$. Then, $\dfrac{m_i}{s_i} \neq 0$ for only finitely many $i \in I$. Let $\Gamma = \left\{i \in I \mid \dfrac{m_i}{s_i} \neq 0\right\}$, let $s = \prod_{i \in \Gamma} s_i$, and set $n_i = \left(\prod_{j \in \Lambda \setminus \{i\}} s_j\right) m_i$ for $i \in \Gamma$ and set $n_i = 0$ if $i \notin \Gamma$. Then, $\phi\left(\dfrac{(n_i)}{s}\right) = \left(\dfrac{n_i}{s}\right) = \left(\dfrac{m_i}{s_i}\right)$ since for $i \in \Gamma$, then $s_i n_i = s_i \left(\prod_{j \in \Lambda \setminus \{i\}} s_j\right) m_i = sm_i$ and for $i \notin \Gamma$, then $n_i = 0$ and there is some $t \in S$ such that $tm_i = 0$ or equivalently, $\dfrac{n_i}{s} = \dfrac{0}{s} = \dfrac{m_i}{s_i}$ and so ϕ is surjective. □

[16] I'm only going to do the Artinian case.

Corollary 228. *If F is a free $R-$module, then F_S is a free R_S-module.*

Proof. Let F be a free $R-$module, so that $F \cong \oplus_{i\in I} R$. Thus, $F_S = \oplus_{i\in I} R_S$ which is a free R_S-module. □

Corollary 229. *If P is a projective $R-$module, then P_S is a projective R_S-module.*

Proof. Since P is projective, then there is some $R-$module, Q, such that $P \oplus Q = F$ where F is a free $R-$module. Then by Lemma 227, $P_S \oplus Q_S \cong F_S$. By the previous corollary, F_S is a free R_S-module, and hence P_S is a projective R_S-module. □

Definition 230. Let $\mu_R(M) := \inf\{n \in \mathbb{N}_0 \mid \text{ there exist } x_1, \ldots, x_n \in M \text{ such that } M = Rx_1 + \ldots + Rx_n\}$. This is the *minimal number of generators of M*.

Note. It is clear that $\mu_R(M) = 0$ if and only if $M = 0$.

Lemma 231 (Nakayama's Lemma). *Let M be a finitely generate $R-$module, and J the Jacobson radical of R. If $M = JM$, then $M = 0$.*

Proof. Suppose $\mu_R(M) = n > 0$. Say $M = Rx_1 + \ldots + Rx_n$. Then, $M = JM = J(Rx_1 + \ldots + Rx_n) = Jx_1 + \ldots + Jx_n$. This gives that $x_n = j_1x_1 + \ldots + j_nx_n$ where $j_k \in J$ for $j = 1, \ldots, n$. Hence, $(1 - j_nx_n = j_1x_1 + \ldots + j_{n-1}x_{n-1}$. Since $j_n \in J$, then $1 - j_n$ is a unit. Hence, $x_n = (1 - j_n)^{-1}j_1x_1 + \ldots + (1 - j_n)^{-1}j_{n-1}x_{n-1}$, so that $Rx_n \in Rx_1 + \ldots + Rx_{n-1}$. This contradicts the minimality of the number of generators, and hence we must have $\mu_R(M) = 0$ and thus $M = 0$ as previously noted. □

Corollary 232. *If $(R, \mathfrak{m})$ is quasi-local, then $J(R) = \mathfrak{m}$. So if M is a finitely generated $R-$module, and $M = \mathfrak{m}M$, then $M = 0$.*

Corollary 233. *Let M be a finitely generated $R-$module, $N \subset M$ be a submodule, and J be the Jacobson radical of R. If $M = N + JM$, then $N = M$.*

Proof. We have $\dfrac{M}{N} = \dfrac{N + JM}{N} = J \cdot \dfrac{M}{N}$. Since M is finitely generated, then M/N is also finitely generated, and hence $M/N = 0$ by Nakayama's Lemma (Lemma 231). Thus, $M = N$ as desired. □

Corollary 234. *Suppose M is a finitely generated $R-$module and $x_1, \ldots, x_n \in M$. Then $x_1, \ldots, x_n$ generate M if and only if $\overline{x_1}, \ldots, \overline{x_n}$ generate M/JM where $\overline{x_i} = x_i + JM$. In particular, this means that $\mu_R(M) = \mu_{R/J}(M/JM)$.*

Proof. If $x_1, \ldots, x_n$ generate M, then we always have $\overline{x_1}, \ldots, \overline{x_n}$ generate M/JM. For the reverse direction, let $N = Rx_1 + \ldots + Rx_n$. Then, $\dfrac{M}{JM} = \dfrac{N + JM}{JM}$. This gives that $M = N + JM$ and so by the previous corollary, we have $N = M$ and so M is generated by $x_1, \ldots, x_n$ as desired. □

Corollary 235. *If $(R, \mathfrak{m})$ is quasi-local, and M is finitely generated, then*

$$\mu_R(M) = \mu_{R/\mathfrak{m}}(M/\mathfrak{m}M) = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M).$$

3.17 Friday 6 April 2012

3.17.1 More on Localization

Definition 236. Let M be a finitely generated $R-$module, and $T \subset M$ a subset. We say T is a *minimal generating set* for M if the elements of T generate M, but not proper subset of T generates M.

Remark 237. Let $(R, \mathfrak{m})$ be a quasi-local ring, M be an $R-$module, and T be a subset of M.

- ▷ Then T is a minimal generating set for M if and only if $\overline{T}$ is a basis for $M/\mathfrak{m}M$.
- ▷ Every minimal generating set for M has the same number of elements.
- ▷ Every generating set contains a minimal generating set.
- ▷ If $x \in M \setminus \mathfrak{m}M$, then x is contained in some minimal generating set.

Example 238. Let $R = \mathbb{Z}/(6)[x]$, and $I = (2, 3x) = (2 - 3x)$. Note here that both $\{2, 3x\}$ and $\{2 - 3x\}$ are minimal generating sets.

Example 239. Let $R = \mathbb{Z}_{(2)}$. Then R is a local ring with maximal ideal $\mathfrak{m} = (2)_{(2)}$. Let $M = \mathbb{Q}$. Then $\mathbb{Q} = \mathfrak{m}\mathbb{Q}$ since $\dfrac{a}{b} = 2 \cdot \dfrac{a}{2b} \in \mathfrak{m}\mathbb{Q}$, but $\mathbb{Q} \neq 0$. Thus, $\mathbb{Q}$ is not a finitely generated $R-$module.

Definition 240. Let $f : M \to N$ be an $R-$module homomorphism and S a multiplicatively closed subset of R. Then define $\frac{f}{1} : M_S \to N_S$ by $\frac{m}{s} \longmapsto \frac{f(m)}{s}$.[17]

Remark 241. Localization is a functor from the usual category of $R-$modules to the usual category of R_S modules. The functor takes the object M to the object M_S and the morphism $f : M \to N$ to the morphism $\frac{f}{1} : M_S \to N_S$.

Proposition 242. *Localization preserves short exact sequences. That is, if $0 \to A \to B \to C \to 0$ is a short exact sequence of $R-$modules, and $S \subset R$ is a multiplicatively closed set, then $0 \to A_S \to B_S \to C_S \to 0$ is a short exact sequence of R_S-modules.*

Proof. Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of $R-$modules and $S \subset R$ a multiplicatively closed subset of R. Note that the maps in the localization of the sequence are $\frac{f}{1} : A_S \to B_S$ and $\frac{g}{1} : B_S \to C_S$. First, we'll show that $\frac{f}{1}$ is injective, so let $\frac{a}{s} \in \ker \frac{f}{1}$. Then, $\frac{f(a)}{s} = 0$ so that there exists some $t \in S$ such that $tf(a) = 0$. Since f is an $R-$module homomorphism, then we have $f(ta) = 0$ so that $ta = 0$ by f being injective. Hence $\frac{a}{s} = 0$ in A_S and $\frac{f}{1}$ is injective. Next, we'll show that $\frac{g}{1}$ is surjective. Let $\frac{c}{s} \in C_S$. Since g is surjective, there exists some $b \in B$ such that $c = g(b)$. Then $\frac{g}{1}\left(\frac{b}{s}\right) = \frac{g(b)}{s} = \frac{c}{s}$ and $\frac{g}{1}$ is surjective. Next, we'll show that image $\frac{f}{1} \subseteq \ker \frac{g}{1}$. Note here that it is enough to show that $\frac{g}{1} \circ \frac{f}{1} = 0$. Since the original sequence is exact, then $gf = 0$, and so $\frac{gf}{1} = \frac{g}{1} \circ \frac{f}{1} = 0$ as well. Finally, we'll show that $\ker \frac{g}{1} \subseteq$ image $\frac{f}{1}$ so that the sequence will be exact at B_S. Let $\frac{b}{s} \in \ker \frac{g}{1}$. Then, $\frac{g(b)}{s} = 0$ so that there exists some $t \in S$ such that $tg(b) = 0$. Since g is an $R-$module homomorphism, we then have that $g(tb) = 0$. Since $\ker(g) = \text{image}(f)$, then there exists some $a \in A$ such that $f(a) = tb$. Thus, $\frac{f}{1}\left(\frac{a}{st}\right) = \frac{f(a)}{st} = \frac{tb}{st} = \frac{b}{s} \in$ image $\frac{f}{1}$ which completes the proof. □

Proposition 243. *Let $(R, \mathfrak{m})$ be a quasi-local ring, and P a finitely generated projective $R-$module. Then P is a free $R-$module.*

Proof. Let $n = \mu_R(P)$, and say $P = Rx_1 + \ldots + Rx_n$ for some $x_1, \ldots, x_n \in P$. Define a map $\phi : R^n \to P$ by $e_i \longmapsto x_i$. Then ϕ is surjective, so we let $K = \ker \phi$ which gives that the following is a short exact sequence of $R-$modules

$$0 \longrightarrow K \longrightarrow R^n \xrightarrow{\phi} P \longrightarrow 0.$$

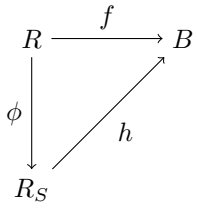
Since P is projective, this sequence splits, and so $R^n \cong P \oplus K$. Then, modding out by $\mathfrak{m}$ gives that $(R/\mathfrak{m})^n \cong R^n/\mathfrak{m}R^n \cong (P \oplus K)/\mathfrak{m}(P \oplus K) \cong P/\mathfrak{m}P \oplus K/\mathfrak{m}K$. Looking at the dimensions of these over $R/\mathfrak{m}$ gives $\dim_{R/\mathfrak{m}}(R/\mathfrak{m})^n = n$ and $\dim_{R/\mathfrak{m}} P/\mathfrak{m}P = n$ since $\mu_R(P) = n$ (see Corollary 235). Thus, $\dim_{R/\mathfrak{m}} K/\mathfrak{m}K = 0$ and so $K = mK$. By Nakayama's Lemma (Lemma 231), we then have that $K = 0$ and hence $P \cong R^n$.[18] □

Remark 244. Let P be a finitely generated projective $R-$module. We can define a map from $\operatorname{Spec} R$ to $\mathbb{N}_0$ by sending the prime ideal q to $\operatorname{rank} P_q$. This makes sense because by Corollary 229, P_q is projective, and by Proposition 243, P_q is free. It can be shown that this map is continuous where the Zarisky topology is used on $\operatorname{Spec} R$ and the discrete topology is used on $\mathbb{N}_0$. Hence, if $\operatorname{Spec} R$ is connected, then the map is constant. Also, R has no nontrivial idempotents if and only if $\operatorname{Spec} R$ is connected. Lastly, it is a fact that if R has no nontrivial idempotents, then the map is constant.

Theorem 245. *Let R be a ring, $S \subset R$ a multiplicatively closed set, and $\phi : R \to R_S$ the cannonical map. Then (R_S, ϕ) has the following universal property: Given any ring, B, and ring homomorphism $f : R \to B$, such that $f(s)$ is a unit in B for every $s \in S$. Then there exists a unique ring homomorphism $h : R_s \to B$ such that the diagram below commutes:*

[17] One could in theory show that this is a well defined R_S-module homomorphism, but I believe that the details aren't tricky.

[18] It is clear that K is finitely generated as $R^n \cong P \oplus K \twoheadrightarrow K$ so that K is a homomorphic image of R^n.



Furthermore, if (T, g) where $g : R \to T$ also has this property, then $T \cong R_S$.

Proof. Given a ring homomorphism $f : R \to B$, define $h : R_S \to B$ by $\frac{r}{s} \longmapsto f(r)f(s)^{-1}$. We first check that h is well defined. So let $\frac{r}{s} = \frac{r'}{s'} \in R_S$. Then there exists some $t \in S$ such that $ts'r = tsr'$. We have then that $h(t)$ is a unit in B, and so $f(t)f(s')f(r) = f(ts'r) = f(tsr') = f(t)f(s)f(r')$ with $f(t)$, $f(s)$, and $f(s')$ units. Thus, $f(r) = f(s')^{-1}f(t)^{-1}f(t)f(s')f(r) = f(s')^{-1}f(t)^{-1}f(t)f(s)f(r') = f(s')^{-1}f(s)f(r')$ and so $f(r)f(s)^{-1} = f(s)^{-1}f(s')^{-1}f(s)f(r') = f(r)f(s')^{-1}$. This shows that h is well defined. We must next check that h is a ring homomorphism, so let $\frac{r}{s}, \frac{r'}{s'} \in R_S$. Then,

$$\begin{aligned} h\left(\frac{r}{s} + \frac{r'}{s'}\right) &= h\left(\frac{s'r + sr'}{ss'}\right) \\ &= f(s'r + sr')f(ss')^{-1} \\ &= \left[f(s')f(r) + f(s)f(r')\right] f(s)^{-1}f(s')^{-1} \\ &= f(r)f(s)^{-1} + f(r')f(s')^{-1} \\ &= h\left(\frac{r}{s}\right) + h\left(\frac{r'}{s'}\right) \end{aligned}$$

and $h\left(\frac{r}{s} \cdot \frac{r'}{s}\right) = h\left(\frac{rr'}{ss'}\right) = f(rr')f(ss')^{-1} = f(r)f(r')f(s)^{-1}f(s')^{-1} = h\left(\frac{r}{s}\right) \cdot h\left(\frac{r'}{s'}\right)$ which shows that h is a ring homomorphism. Let $r \in R$. Then $(h \cdot \phi)(r) = h(\phi(r)) = h\left(\frac{r}{1}\right) = f(r)f(1)^{-1} = f(r)$ which shows that the diagram in question commutes. Now, if $h' : R_S \to B$ is also a well defined ring homomorphism such that $h'\phi = f$, then for any $r \in R$, we have $f(r) = h'(\phi(r)) = h'\left(\frac{r}{1}\right)$. Also, for any $s \in S$, then $f(s)$ is a unit and $\phi(s)$ is a unit, and so $f(s)^{-1} = h'(\phi(s))^{-1} = h'\left(\frac{s}{1}\right)^{-1} = h'\left(\frac{s^{-1}}{1}\right) = h'\left(\frac{1}{s}\right)$ since h' is a ring homomorphism and $\frac{s}{1}$ is a unit in R_S. Thus, since h' is a ring homomorphism, we must have that $h'\left(\frac{r}{s}\right) = f(r)f(s)^{-1}$ and hence h is unique. The uniqueness of R_S is the same argument as it always is to see that objects in a category satisfying universal properties are unique. For an explicit description, see the Aside near the top of page 2 of the 901 notes. □

3.18 Monday 9 April 2012

3.18.1 Useful facts about localization

Proposition 246. *If $N \subseteq M$ are $R-$modules and S is a multiplicatively closed subset of R, then $(M/N)_S \cong M_S/N_S$ as R_S-modules.*

Proof. We have an exact sequence $0 \to N \to M \to M/N \to 0$ where the map from N to M is the inclusion map. Localizing at S gives the exact sequence $0 \to N_S \to M_S \to (M/N)_S \to 0$ and hence $M_S/N_S \cong (M/N)_S$. □

Corollary 247. *If $I \subseteq R$ is an ideal and S is a multiplicatively closed subset of R, let $\overline{S} = \{\overline{s} = s + I \mid s \in S\}$ and note that $\overline{S} \subseteq R/I$ is multiplicatively closed. Then $(R/I)_{\overline{S}} \cong R_S/I_S$ as rings. The map here is given by $\frac{\overline{r}}{\overline{s}} \longmapsto \overline{\frac{r}{s}}$.*

Remark 248. As a special case,let $P \in \operatorname{Spec} R$. Then the residue field of R_P is $R_P/P_P \cong (R/P)_{(0)} = Q(R/P)$, which is the field of fractions of R/P.

Chapter 4

Post-Exam 2 Material

4.1 Monday 9 April 2012

4.1.1 Tensor Products

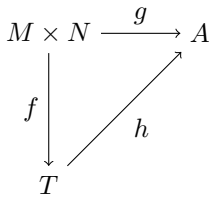
Definition 249. Let M, N, A be $R-$modules. We say a map $f : M \times N \to A$ is $R-$*bilinear* if for every $m, m' \in M$, $n, n' \in N$ and $r \in R$, we have the following:

- $f(m + m', n) = f(m, n) + f(m', n)$,
- $f(m, n + n') = f(m, n) + f(m, n')$, and
- $f(rm, n) = f(m, rn) = rf(m, n)$.

Example 250. These examples are easily seen to be bilinear.[1]

- Let S be an $R-$algebra. Then the multiplication map $\cdot : S \times S \to S$ given by $(a, b) \longmapsto ab$ is $R-$bilinear.
- The map $R_S \times M \to M_S$ given by $\left(\frac{r}{s}, m\right) \longmapsto \frac{rm}{s}$ is $R-$bilinear.
- The map $R/I \times M \to M/IM$ given by $(\overline{r}, m) \longmapsto \overline{rm}$ is $R-$bilinear.

Theorem 251. *Let M and N be $R-$modules. Then there exists an $R-$module T together with an $R-$bilinear map $f : M \times N \to T$ with the following universal property: Given any $R-$bilinear map $g : M \times N \to A$ where A is also an $R-$modules, then there exists a unique $R-$module homomorphism $h : T \to A$ such that the following diagram commutes:*



Furthermore, if $f' : M \times N \to T'$ also has this property, then $T \cong T'$.

Proof. Once we have the existence of such a module T, the uniqueness of T is the same argument as it always is to see that objects in a category satisfying universal properties are unique. For an explicit description, see the Aside near the top of page 2 of the 901 notes. For this proof, we'll explicitly construct T. Let F be a free $R-$module with basis $S = \{e_{(m,n)} \mid (m, n) \in M \times N\}$. Then S is in bijection with $M \times N$ and every element of F can be written uniquely as $\sum_{i=1}^{t} r_i e_{(m_i,n_i)}$ where $r_i \in R$. Let U be the submodule of F which is generated by all elements of the following forms:

- $e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}$,
- $e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}$,
- $e_{(rm,n)} - re_{(m,n)}$, and
- $e_{(m,rn)} - re_{(m,n)}$

where $m, m' \in M$, $n, n' \in N$, and $r \in R$. Set $T = F/U$ and let $m \otimes n$ denote $e_{(m,n)} + U \in T = F/U$. Using the above definitions, we see that $(m+m') \otimes n = e_{(m+m',n)} + U = (e_{(m,n)} + e_{(m',n)}) + U = (e_{(m,n)} + U) + (e_{(m',n)} + U) = m \otimes n + m' \otimes n$. Similarly, $m \otimes (n + n') = m \otimes n + m \otimes n'$, and $(rm) \otimes n = r(m \otimes n) = m \otimes (rn)$. It is clear that T is an $R-$module since it is a quotient of a free $R-$module. Define $f : M \times N \to T$ by $(m, n) \longmapsto m \otimes n$. By construction of T it is clear that f is $R-$bilinear. It remains then to check the universal property, so let $g : M \times N \to A$ be an $R-$bilinear map. Define an $R-$module homomorphism $\widetilde{h} : F \to A$ by $e_{(m,n)} \longmapsto g(m, n)$. This is well defined since F is a free $R-$module. Since g is $R-$bilinear, then $U \subseteq \ker \widetilde{h}$. For example, $\widetilde{h}(e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}) = g(m, n + n') - g(m, n) - g(m, n')$ and this is equal to 0 because g is $R-$bilinear. Therefore, $\widetilde{h}$ induces an $R-$module homomorphism $h : T \to A$ which is given

[1] The details aren't worth doing.

by $m \otimes n \longmapsto g(m,n)$ and this map is well defined. The diagram in question commutes by definition of h. So suppose there is a second map $h' : T \to A$ which also satisfies $g = h'f$. Then $h'(m \otimes n) = h'f(m,n) = g(m,n) = h(m \otimes n)$ and so h is unique because the set $\{m \otimes n \mid m \in M, n \in N\}$ generates T. □

Definition 252. The module T in the above theorem is called the *tensor product of M and N over R* and is denoted $M \otimes_R N$.

4.2 Wednesday 11 April 2012

4.2.1 Tensor Product Properties

Remark 253. If $M = Ru_1 + \ldots + Ru_t$ and $N = Rw_1 + \ldots + Rw_s$, then $M \otimes_R N = \sum_{i,j} R(u_i \otimes w_j)$. More precisely, elements of M are of the form $m = \sum_{i=1}^{t} r_i u_i$ and elements of N are of the form $n = \sum_{j=1}^{s} r'_j w_j$ so that the tensor of m and n is $m \otimes n = \left(\sum_{i=1}^{t} r_i u_i\right) \otimes \left(\sum_{j=1}^{s} r'_j w_j\right) = \sum_{i,j} r_i r'_j (u_i \otimes w_j)$. Thus, $\mu_R(M \otimes_R N) \leq \mu_R(M)\mu_R(N)$.[2] Thus, if M and N are finitely generated, we have that $M \otimes_R N$ is also finitely generated.

Proposition 254. *Let M, N, L, and M_i for $i \in \Lambda$ be $R-$modules, S a multiplicatively closed subset of R, and I an ideal of R. Then we have the following isomorphisms along with the maps giving the isomorphisms:*

1. $M \otimes_R N \cong N \otimes_R M$
   $m \otimes n \longmapsto n \otimes m$
2. $R \otimes_R M \cong M$
   $r \otimes m \longmapsto rm$
3. $R_S \otimes_R M \cong M_S$
   $\frac{r}{s} \otimes m \longmapsto \frac{rm}{s}$
4. $R/I \otimes_R M \cong M/IM$
   $\overline{r} \otimes m \longmapsto \overline{rm}$
5. $\left(\bigoplus_{i\in\Lambda} M_i\right) \otimes_R N \cong \bigoplus_{i\in\Lambda} (M_i \otimes_R N)$
   $(m_i) \otimes n \longmapsto (m_i \otimes n)$
6. $(M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L)$
   $(m \otimes n) \otimes \ell \longmapsto m \otimes (n \otimes \ell)$

Proof. The proofs of these statements are all very similar in form. We'll do all the details for 3 and the important details for 4. Also, property 6 above will be proved in more generality in Proposition 280.

3. Define a map $\widetilde{f} : R_S \times M \to M_S$ by $\left(\frac{r}{s}, m\right) \longmapsto \frac{rm}{s}$. We first need to show that $\widetilde{f}$ is well defined, so suppose that $\frac{r}{s} = \frac{r'}{s'}$. Then there exists some $t \in S$ such that $ts'r = tsr'$. Thus, $ts'rm = tsr'm$ so that $\frac{rm}{s} = \frac{r'm}{s'}$ which shows that $\widetilde{f}$ is well defined. Next, we must show that $\widetilde{f}$ is bilinear, so let $\frac{r}{s}, \frac{r'}{s'} \in R_S$, $m, m' \in M$, and $a \in R$. Then we have the following:

$$\widetilde{f}\left(\frac{r}{s} + \frac{r'}{s'}, m\right) = \widetilde{f}\left(\frac{s'r + sr'}{ss'}, m\right) = \frac{(s'r + sr')m}{ss'} = \frac{s'rm + sr'm}{ss'} = \frac{rm}{s} + \frac{r'm}{s'} = \widetilde{f}\left(\frac{r}{s}, m\right) + \widetilde{f}\left(\frac{r'}{s'}, m\right),$$

$$\widetilde{f}\left(\frac{r}{s}, m + m'\right) = \frac{r(m+m')}{s} = \frac{rm}{s} + \frac{rm'}{s} = \widetilde{f}\left(\frac{r}{s}, m\right) + \widetilde{f}\left(\frac{r}{s}, m'\right), \text{ and}$$

$$\widetilde{f}\left(a \cdot \frac{r}{s}, m\right) = \widetilde{f}\left(\frac{ar}{s}, m\right) = \frac{arm}{s} = \frac{ram}{s} = \widetilde{f}\left(\frac{r}{s}, am\right) = a\frac{rm}{s} = a\widetilde{f}\left(\frac{r}{s}, m\right).$$

Thus, by definition of the tensor product, there is an $R-$module homomorphism $f : R_S \otimes_R M \to M_S$ such that the diagram below commutes where the map $\phi : R_S \times M \to R_S \otimes_R M$ is the canonical map given by $\left(\frac{r}{s}, m\right) \longmapsto \frac{r}{s} \otimes m$:

$$\begin{array}{ccc} R_S \times M & \xrightarrow{\widetilde{f}} & M_S \\ \Big\downarrow{\scriptstyle \phi} & \nearrow{\scriptstyle f} & \\ R_S \otimes_R M & & \end{array}$$

[2] I believe that Tom said that we get equality when R is local and M, N are finitely generated.

The map f then must act as $f\left(\frac{r}{s}\otimes m\right)=\frac{rm}{s}$ by commutativity of the diagram. In order to show that f is an isomorphism, we'll show that it has an inverse. So, let $g:M_S\to R_S\otimes_R M$ be given by $\frac{m}{s}\longmapsto\frac{1}{s}\otimes m$. First, we have that for any $\frac{m}{s},\frac{m'}{s'}\in M_S$ and any $r\in R$, that

$$\begin{aligned}
g\left(\frac{m}{s}+\frac{m'}{s'}\right) &= g\left(\frac{s'm+sm'}{ss'}\right)\\
&= \frac{1}{ss'}\otimes(s'm+sm')\\
&= \frac{1}{ss'}\otimes s'm+\frac{1}{ss'}\otimes sm'\\
&= \frac{s'}{ss'}\otimes m+\frac{s}{ss'}\otimes m'\\
&= \frac{1}{s}\otimes m+\frac{1}{s'}\otimes m'\\
&= g\left(\frac{m}{s}\right)+g\left(\frac{m'}{s'}\right)
\end{aligned}$$

and

$$g\left(r\frac{m}{s}\right)=g\left(\frac{rm}{s}\right)=\frac{1}{s}\otimes rm=\frac{r}{s}\otimes m=r\left(\frac{1}{s}\otimes m\right)=rg\left(\frac{m}{s}\right),$$

so that g is an $R-$module homomorphism. Next, we need to show that g is well defined. Since it is an $R-$module homomorphism, then if $\frac{m}{s}=\frac{m'}{s'}$, we'll get that $g\left(\frac{m}{s}-\frac{m'}{s'}\right)=0$ only if g is well defined, so it is sufficient to show that if $\frac{m}{s}=0$, then $g\left(\frac{m}{s}\right)=0$. To that end, suppose that $\frac{m}{s}=0$. Then by definition, there exists some $t\in S$ such that $tm=0$. Now, $\frac{1}{s}\otimes m=\frac{t}{st}\otimes m=\frac{1}{st}\otimes tm=\frac{1}{st}\otimes 0=0$ so that g is indeed well defined. It then only remains to show that g and f are inverses. It is enough to show this on a generating set since they're both $R-$module homomorphisms. So, let $\frac{r}{s}\otimes m\in R_S\otimes_R M$ and $\frac{m}{s}\in M_S$. Then, we have

$$(g\circ f)\left(\frac{r}{s}\otimes m\right)=g\left(f\left(\frac{r}{s}\otimes m\right)\right)=g\left(\frac{rm}{s}\right)=\frac{1}{s}\otimes rm=\frac{r}{s}\otimes m$$

and

$$(f\circ g)\left(\frac{m}{s}\right)=f\left(g\left(\frac{m}{s}\right)\right)=f\left(\frac{1}{s}\otimes m\right)=\frac{m}{s}$$

so that $f\circ g=id_{M_S}$ and $g\circ f=id_{R_S\otimes_S M}$ as desired.

4. Define $\widetilde{f}:R/I\times M\to M/IM$ by $(\overline{r},m)\longmapsto\overline{rm}$. It is easy to check that $\widetilde{f}$ is well defined and $R-$bilinear. Thus, it induces an $R-$module homomorphism $f:R/I\otimes_R M\to M/IM$ where $\overline{r}\otimes m\longmapsto\overline{rm}$. Next, define a map $g:M\to R/I\otimes_R M$ by $m\longmapsto\overline{1}\otimes m$. It is easy to check that g is an $R-$module homomorphism. If $x\in IM$, then we can write $x=\sum_{j=1}^n r_jm_j$ for some $r_j\in I$ and $m_j\in M$. Then, $g(x)=\overline{1}\otimes x=\overline{1}\otimes\sum r_jm_j=\sum(\overline{r_j}\otimes m_j)=\sum(0\otimes m_j)=0$ so that $IM\subseteq\ker(g)$. Thus, we have an induced $R-$module homomorphism $\overline{g}:M/IM\to R/I\otimes_R M$ which is given by $\overline{m}\longmapsto\overline{1}\otimes m$. It is easy to check that f and $\overline{g}$ are inverses.

□

Remark 255. If F is a free $R-$module of rank n and G is a free $R-$module of rank m, then

$$F\otimes_R G\cong R^n\otimes_R R^m\cong\bigoplus_{i=1}^n(R\otimes_R R^m)\cong\bigoplus_{i=1}^n R^m\cong R^{mn}$$

so that $F\otimes_R G$ is a free $R-$module of rank mn. More generally, if $\{u_i\}_{i\in I}$ is a basis for F and $\{v_j\}_{j\in J}$ is a basis for G, then $\{u_i\otimes v_j\}_{(i,j)\in I\times J}$ is a basis for $F\otimes_R G$.

4.3 Friday 13 April 2012

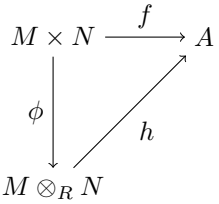
4.3.1 More on Tensor Products

Remark 256. If M and N are $R-$modules, and $m \in M$, $n \in N$, it is a hard question in general to determine when $m \otimes n = 0$ in $M \otimes_R N$.

Lemma 257. *Let M, N be $R-$modules and $m \in M$, $n \in N$. Then $m \otimes n = 0$ if and only if $f(m,n) = 0$ for every $R-$bilinear map $f : M \times N \to A$ where A is an $R-$module.*

Proof. ($\Leftarrow$) The canonical map $\phi : M \times N \to M \otimes_R N$ given by $(m,n) \longmapsto m \otimes n$ is $R-$bilinear, so if $f(m,n) = 0$ for every such map f, then $m \otimes n = \phi(m,n) = 0$.

($\Rightarrow$) If $f : M \times N \to A$ is $R-$bilinear, then there exists an $R-$module homomorphism $h : M \otimes_R N \to A$ such that the following diagram commutes.



Thus, $f(m,n) = h(m \otimes n) = h(0) = 0$ as desired. □

Example 258. Consider $2 \otimes \overline{1}$ in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. We have

$$2 \otimes \overline{1} = 2 \cdot 1 \otimes \overline{1} = 1 \otimes 2 \cdot \overline{1} = 1 \otimes \overline{2} = 1 \otimes \overline{0} = 0.$$

Now, consider $2 \otimes \overline{1}$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. Here, we have that $2 \otimes \overline{1} \neq 0$ and we can show this using the previous lemma. Let $f : 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be given by $(2n, \overline{a}) \longmapsto \overline{na}$. It is easy to check that f is $\mathbb{Z}-$bilinear. Also, $f(2, \overline{1}) = \overline{1} \neq 0$ and so $2 \otimes \overline{1} \neq 0$ in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

Remark 259. The lesson to learn from the previous example is that if $M' \subseteq M$ is a submodule, then $M' \otimes_R N$ cannot generally be identified with a submodule of $M \otimes_R N$ since the "inclusion" map may not be injective.

4.3.2 Functors on Module Categories

Notation. We will use the notation $\mathbf{R-mod}$ to denote the category of $R-$modules where the objects are $R-$modules and the morphisms are $R-$module homomorphism.

Note. If M, N are $R-$modules, then $\mathrm{Hom}_R(M,N) := \{f : M \to N \mid f \text{ is an } R-\text{module homomorphism}\}$ is an $R-$module.

Recall. A covariant functor is a map $F : \mathbf{R-mod} \to \mathbf{S-mod}$ such that $F(M)$ is an $S-$module for every $R-$module M, and given morphisms $f : M \to N$ and $g : N \to L$ in $\mathbf{R-mod}$, then $F(gf) = F(g)F(f)$. Also, we must have that $F(id_M) = id_{F(M)}$.

Proposition 260. *Let $f : M \to N$ and $g : A \to B$ be $R-$module homomorphisms. Then there is an $R-$module homomorphism $f \otimes g : M \otimes_R A \to N \otimes_R B$ such that $m \otimes a \longmapsto f(m) \otimes g(a)$. We say that $f \otimes g$ is the tensor product of f and g.*

Proof. Define $f \times g : M \times A \to N \otimes_R B$ by $(m,a) \longmapsto f(m) \otimes g(b)$. It is easy to show that $f \times g$ is $R-$bilinear. Thus, there is an induced $R-$linear homomorphism $f \otimes g : M \otimes_R A \to N \otimes_R B$ and it is given by $m \otimes a \longmapsto f(m) \otimes g(a)$. □

Definition 261. Given an $R-$module, M, we can define a covariant functor $F_M : \mathbf{R-mod} \to \mathbf{R-mod}$ by $F_M(N) = M \otimes_R N$ and if $g : N \to L$ is a morphism in $\mathbf{R-mod}$, then $F_M(g) = id_M \otimes g : M \otimes_R N \to M \otimes_R L$. The typical notation for this functor is $M \otimes_R -$.

Remark 262. The functor $- \otimes_R M$ can be similarly defined, and is also covariant.

Definition 263. A functor $F : \mathbf{R-mod} \to \mathbf{S-mod}$ is called *additive* if for $R-$modules M, N, and $f, g \in \mathrm{Hom}_R(M,N)$, then $F(f+g) = F(f) + F(g)$.

Exercise. If F is an additive functor, then $F(0) = 0$ on both maps and objects.[3]

Note. The functors $M \otimes_R -$ and $- \otimes_R M$ are additive functors.

[3] There was some argument about whether or not this is actually true, and so I should do this exercise soon!

Notation. Let A be an $R-$module, and $x \in R$. Then $\mu_{x,A}$ is the map $A \to A$ given by $a \longmapsto xa$.

Definition 264. A functor $F : \mathbf{R-mod} \to \mathbf{S-mod}$ is called *multiplicative* if given an $R-$module, M, and any $r \in R$, then $F(\mu_{r,M}) = \mu_{r,F(M)}$.

Note. The functors $M \otimes_R -$ and $- \otimes_R M$ are multiplicative.

Proposition 265. *Let $R \to S$ be a ring homomorphism, and let M be an $S-$module.*[4] *For any $R-$module, N, then $M \otimes_R N$ is an $S-$module via $s \cdot (m \otimes n) := (sm) \otimes n$.*

Proof. Let $s \in S$, and let $f_s : M \times N \to M \otimes_R N$ be given by $(m, n) \longmapsto (sm) \otimes n$. This is $R-$bilinear and so it induces an $R-$module homomorphism $M \otimes_R N \to M \otimes_R N$. □

Remark 266. If in the previous proposition, we choose $M = S$, then we see that $S \otimes_R -$ is an additive and multiplicative functor. Moreover, $S \otimes_R M$ is an $S-$module.

Example 267. These are some of the most commonly used[5] additive and multiplicative functors in commutative algebra.

- ▷ **Modding out:** Let I be an ideal of R. Then $R/I \otimes_R - : \mathbf{R-mod} \to \mathbf{R/I-mod}$ is the functor which takes the $R-$module, M to $R/I \otimes_R M \cong M/IM$.
- ▷ **Localization:** Let S be a multiplicatively closed subset of R. Then $R_S \otimes_R - : \mathbf{R-mod} \to \mathbf{R_S-mod}$ is the functor which takes the $R-$module, M to $R_S \otimes_R M \cong M_S$.

Definition 268. A covariant additive functor F on module categories is called *right exact* if whenever

$$L \xrightarrow{\quad f \quad} M \xrightarrow{\quad g \quad} N \longrightarrow 0$$

is exact, then

$$F(L) \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(N) \longrightarrow 0$$

is also exact.

4.4 Monday 16 April 2012

4.4.1 Tensor Product is a Right Exact Functor

Theorem 269. *The functor $M \otimes_R -$ is right exact.*

Proof. Let

$$A \xrightarrow{\quad f \quad} B \xrightarrow{\quad g \quad} C \longrightarrow 0$$

be an exact sequence of $R-$modules, and let M be an $R-$module. We need to show that

$$M \otimes_R A \xrightarrow{1 \otimes f} M \otimes_R B \xrightarrow{1 \otimes g} M \otimes_R C \longrightarrow 0$$

is exact. We'll start by showing that $1 \otimes g$ is surjective. So let $\sum_{i=1}^{n} m_i \otimes c_i \in M \otimes_R C$. Since g is surjective, then for each $i \in \{1, \ldots, n\}$ there exists $b_i \in B$ such that $g(b_i) = c_i$. Thus, $(1 \otimes g)\left(\sum_{i=1}^{n} m_i \otimes b_i\right) = \sum_{i=1}^{n} m_i \otimes g(b_i) = \sum_{i=1}^{n} b_i \otimes c_i$ as desired. Next, we have that $gf = 0$ since the original sequence was exact and so we have $(1 \otimes g)(1 \otimes f) = 1 \otimes (gf) = 1 \otimes 0 = 0$ which gives that $\text{image}(1 \otimes f) \subseteq \ker(1 \otimes g)$. Finally, let $E = \text{image}(1 \otimes f) \subseteq M \otimes_R B$. As $E \subseteq \ker(1 \otimes g)$, we have an induced map $h := \overline{1 \otimes g} : (M \otimes_R B)/E \to M \otimes_R C$ which is given by $\overline{m \otimes b} \longmapsto m \otimes g(b)$. Note that h is surjective by definition. Hence, it suffices to show that h is an isomorphism, and so we'll produce an inverse for h. To that end, define $\alpha : M \times C \to (M \otimes_R B)/E$ by $(m, c) \longmapsto \overline{m \otimes b}$ where $b \in B$ is chosen so that $g(b) = c$. This can be done since g is surjective, but we must show that α is independent of the choice of b. If $g(b) = g(b') = c$, then $g(b - b') = 0$ which gives that $b - b' \in \ker(g) = \text{image}(f)$ so there exists some $a \in A$ such that $f(a) = b - b'$. Thus, $m \otimes b - m \otimes b' = m \otimes (b - b') = m \otimes f(a) = (1 \otimes f)(m \otimes a) \in \text{image}(1 \otimes f) = E$ and hence $\overline{m \otimes b} = \overline{m \otimes b'}$. It is easy to show that α is $R-$bilinear, and so there is an induced map $\widetilde{\alpha} : M \otimes_R C \to$

[4] And so M will also be an $S-$module.
[5] I believe.

$M \otimes_R B/E$ such that $\widetilde{\alpha}(m \otimes c) = \overline{m \otimes b}$ for any $b \in B$ with $g(b) = c$. If $\overline{m \otimes b} \in M \otimes_R B/E$, then $\widetilde{\alpha}h(\overline{m \otimes b}) = \widetilde{\alpha}(m \otimes g(b)) = \overline{m \otimes b}$ so that $\widetilde{\alpha}h = id_{M \otimes_R B/E}$ on a generating set, and hence on all of $M \otimes_R B/E$. Similarly, if $m \otimes c \in M \otimes_R C$, then $h\widetilde{\alpha}(m \otimes c) = h(m \otimes b) = m \otimes g(b) = m \otimes c$ for any $b \in B$ such that $g(b) = c$. Thus, $h\widetilde{\alpha} = id_{M \otimes_R C}$ on a generating set, and hence on all of the module. Thus, h is an isomorphism, and so $\operatorname{image} 1 \otimes f = E = \ker 1 \otimes g$ as desired. □

Remark 270. The functor $M \otimes_R -$ does not necessarily preserve injections!

Example 271. It is clear that the inclusion map $i : 2\mathbb{Z} \to \mathbb{Z}$ is injective. However, when we apply the functor $- \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ we obtain the map $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ which takes $\overline{1} \otimes 2$ to $\overline{1} \otimes 2$. In Example 258 we showed that $\overline{1} \otimes 2$ is nonzero in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ but is equal to zero in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ and so this map is not injective.

4.4.2 Flat Modules

Definition 272. An $R-$module M is called *flat* (over R) if $M \otimes_R -$ preserves injections, or equivalently we can say that it is an exact functor.

Lemma 273. *Suppose the fullowing diagram commutes*

$$\begin{array}{ccccc} A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' \end{array}$$

and f, g, h are isomorphism. Then the top row is exact if and only if the bottom row is exact.

Proof. Since f, g, h are isomorphisms, it is enough to prove that the bottom row is exact if the top row is exact. Let $b' \in \operatorname{image} \alpha'$. Then there exists some $a' \in A'$ such that $\alpha'(a') = b'$. Since f is an isomorphism, there is some $a \in A$ such that $f(a) = a'$. Then as the top row is exact, we have that $\beta(\alpha(a)) = 0 \in C$. As h is an isomorphism, then $h(\beta(\alpha(a))) = 0$. Now, by commutativity of the diagram, $h\beta\alpha = \beta'\alpha' f$ and so $\beta'\alpha' f(a) = 0$ as well. Note then that $\beta'(\alpha'(f(a))) = \beta'(\alpha'(a')) = \beta'(b')$. Thus, $b' \in \ker \beta'$.

Next, let $b' \in \ker(\beta')$. As g is an isomorphism, there is some $b \in B$ such that $g(b) = b'$. Also, as $b' \in \ker \beta'$, then $\beta'(b') = 0$. As h is an isomorphism, then $h^{-1}(\beta'(b')) = 0$ as well. Note that $h^{-1}\beta' g = \beta$ by the commutativity of the right square, and so $\beta(b) = h^{-1}(\beta'(g(b))) = h^{-1}(\beta'(b')) = h^{-1}(0) = 0$. thus, $b \in \ker \beta = \operatorname{image} \alpha$ so there exists some $a \in A$ such that $\alpha(a) = b$. Let $a' = f(a)$. Then, by the commutativity of the let square, we have that $\alpha'(a') = \alpha'(f(a)) = g(\alpha(a)) = g(b) = b'$ so that $b' \in \operatorname{image} \alpha'$. □

Lemma 274. *Let $\{A_i\}_{i \in \Lambda}$ be a family of $R-$modules. Then A_i is flat for every $i \in \Lambda$ if and only if $\bigoplus_{i \in \Lambda} A_i$ is flat.*

Proof. Let

$$0 \longrightarrow M \xrightarrow{f} N$$

be exact, and consider the commutative diagram below:

$$\begin{array}{ccccc} 0 \longrightarrow \left(\bigoplus_{i \in \Lambda} A_i\right) \otimes_R M & \xrightarrow{1_A \otimes f} & \left(\bigoplus_{i \in \Lambda} A_i\right) \otimes_R N \\ \downarrow & & \downarrow \\ 0 \longrightarrow \bigoplus_{i \in \Lambda} (A_i \otimes_R M) & \xrightarrow{1_{A_i} \otimes f'} & \bigoplus_{i \in \Lambda} (A_i \otimes_R N) \end{array}$$

where 1_A is the identity map on $\bigoplus_{i \in \Lambda} A_i$ and 1_{A_i} is the identity map on A_i. The vertical maps are the canonical isomorphisms as given in Proposition 254. Chasing the element $(a_i) \otimes m$ through the diagram gives:

$$\begin{array}{ccc} (a_i \otimes m) & \longmapsto & (a_i) \otimes f(m) \\ \downarrow & & \downarrow \\ (a_i \otimes m) & \longmapsto & (a_i \otimes f(m)) \end{array}$$

so that the diagram commutes. Then we have that $\bigoplus_{i \in \Lambda} A_i$ is flat if and only if the top row is exact, which by Lemma 273 is if and only if the bottom row is exact. In turn, the bottom row is exact if and only if it is exact on each component, and hence if and only if A_i is flat for all $i \in \Lambda$. □

Proposition 275. *Every projective $R-$module is flat.*

Proof. Let P be a projective $R-$module. Then there exists some $R-$module, Q, and a free $R-$module, F, such that $F \cong P \oplus Q$. Thus, it is enough to show that every free module is flat. However, since every free $R-$module is just a direct sum of some copies of R, then it is sufficient to show that R is flat. Let

$$0 \longrightarrow M \xrightarrow{f} N$$

be exact. Then consider the following diagram where the vertical maps are given by the canonical isomorphisms in Proposition 254.

$$\begin{array}{ccccc} 0 & \longrightarrow & R \otimes_R M & \xrightarrow{1 \otimes f} & R \otimes_R N \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & M & \xrightarrow{f} & N \end{array}$$

It is easy to show that the diagram commutes, and the bottom row is already exact. Thus, by Lemma 273, the top row is exact and so R is flat, which completes the proof. □

Proposition 276. *Let S be a multiplicatively closed subset of R. Then R_S is a flat $R-$module.*

Proof. Let

$$0 \longrightarrow M \xrightarrow{f} N$$

be exact. Then consider the following diagram where the vertical maps are given by the canonical isomorphisms in Proposition 254.

$$\begin{array}{ccccc} 0 & \longrightarrow & R_S \otimes_R M & \xrightarrow{1 \otimes f} & R_S \otimes_R M \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & M_S & \xrightarrow{\frac{f}{1}} & N_S \end{array}$$

The diagram is easily shown to commute. Also, the bottom row is exact since localization is an exact functor. Thus, the top row is exact, and so R_S is a flat $R-$module. □

Definition 277. A ring homomorphism $\phi : R \to S$ is called a *flat ring map* if S is a flat $R-$module.

Example 278. The following ring homomorphisms are flat ring maps:

- ▷ The identity map. $id : R \to R$.
- ▷ The canonical localization map. $\phi : R \to R_S$.
- ▷ The inclusion map for adjoining an indeterminant. $\phi : R \to R[x]$.
- ▷ The completion map. $\phi : R \to \hat{R}$.

▷ In a local ring $(R, \mathfrak{m})$ of characteristic $p > 0$, the Frobenius map $f : R \to R$ given by $r \longmapsto r^p$ is flat if and only if R is a regular local ring.[6] Which happens if and only if $\mu_R(\mathfrak{m}) = \dim R$.

4.5 Wednesday 18 April 2012

4.5.1 More Tensor Products

Example 279. How many distinct elements are in the $\mathbb{Z}-$module $\mathbb{Z}_{45} \otimes_{\mathbb{Z}} \mathbb{Z}^3 \otimes_{\mathbb{Z}} \mathbb{Z}/100\mathbb{Z}$? This question is easily answered by using the isomorphisms in Proposition 254. Note that in general $(R/I)_S \cong R/I \otimes_R R_S \cong R_S/I_S$. We have

$$\begin{aligned}
\mathbb{Z}_{45} \otimes_{\mathbb{Z}} \mathbb{Z}^3 \otimes_{\mathbb{Z}} \mathbb{Z}/100\mathbb{Z} &\cong \mathbb{Z}^3 \otimes_{\mathbb{Z}} (\mathbb{Z}_{45} \otimes_{\mathbb{Z}} \mathbb{Z}/100\mathbb{Z}) \\
&\cong \mathbb{Z}^3 \otimes_{\mathbb{Z}} (\mathbb{Z}_{45}/100\mathbb{Z}_{45}) \\
&\cong \mathbb{Z}^3 \otimes_{\mathbb{Z}} (\mathbb{Z}_{45}/4\mathbb{Z}_{45}) \\
&\cong \mathbb{Z}^3 \otimes_{\mathbb{Z}} (\mathbb{Z}/4\mathbb{Z})_{\overline{45}} \\
&\cong \mathbb{Z}^3 \otimes_{\mathbb{Z}} (\mathbb{Z}/4\mathbb{Z}) \\
&\cong (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/4\mathbb{Z})^3 \\
&\cong (\mathbb{Z}/4\mathbb{Z})^3
\end{aligned}$$

using the fact that $100 = 5^2 \cdot 4$, that $\dfrac{9^2}{45^2} = \dfrac{1}{5^2}$ so 5^2 is a unit in $\mathbb{Z}_{45}$, and also that $45 \equiv 1$ in $\mathbb{Z}/4\mathbb{Z}$. Hence, $\mathbb{Z}_{45} \otimes_{\mathbb{Z}} \mathbb{Z}^3 \otimes_{\mathbb{Z}} \mathbb{Z}/100\mathbb{Z}$ has $4^3 = 64$ distinct elements.

Note. If $R \to S$ is a ring homomorphism, A is an $R-$module, and B is an $S-$module, then $A \otimes_R B$ is an $S-$module via $s \cdot (a \otimes b) = a \otimes (sb)$.

Proposition 280. *Let $R \to S$ be a ring homomorphism, A be an $R-$module, and B, C be $S-$modules. Note that B, C are also $R-$modules via the homomorphism. Then*

$$A \otimes_R (B \otimes_S C) \cong (A \otimes_R B) \otimes_S C$$

as $S-$modules and the isomorphism is given by $a \otimes (b \otimes c) \longmapsto (a \otimes b) \otimes c$.

Proof. Fix some $a \in A$ and define a map $f_a : B \times C \to (A \otimes_R B) \otimes_S C$ which is given by $(b, c) \longmapsto (a \otimes b) \otimes c$. It is easy to show that f_a is $S-$bilinear and so there is an induced $S-$module homomorphism $\widetilde{f_a} : B \otimes_S C \to (A \otimes_R B) \otimes_S C$ under which $b \otimes c \longmapsto (a \otimes b) \otimes c$. Now, define a map $g : A \times (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$ by $(a, x) \longmapsto \widetilde{f_a}(x)$. In particular $g(a, b \otimes c) = (a \otimes b) \otimes c$. It is easy to see than g is $R-$bilinear, and so there is an induced $R-$module homomorphism $\widetilde{g} : A \otimes_R (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$ under which $a \otimes (b \otimes c) \longmapsto (a \otimes b) \otimes c$. Note that $\widetilde{g}(s \cdot x) = s\widetilde{g}(x)$ is clear on a generating set, and so $\widetilde{g}$ is actually $S-$linear. Similarly, one can define an $S-$linear map in the other direction, and they'll clearly compose to the identity on a generating set, and hence will be inverses. □

Example 281. Let M, N be $R-$modules, and I an ideal of R such that $IM = IN = 0$. Then note that for $A = M$ or $A = N$, we have $A \otimes_R R/I \cong A/IA \cong A/0 \cong A$ since $IA = 0$. Then,

$$M \otimes_R N \cong (M \otimes_{R/I} R_I) \otimes_R N \cong M \otimes_{R/I} (R/I \otimes_R N) \cong M \otimes_{R/I} N$$

by using the properties in Proposition 254.

Example 282. The exercise on the homework which states "Let $(R, \mathfrak{m})$ be a quasi-local ring and M, N finitely generated $R-$modules. Then $M \otimes_R N = 0$ if and only if $M = 0$ or $N = 0$." is false if R is not quasi local or if M or N is not finitely generated. In particular, note that $\mathbb{Z}/2\mathbb{Z} \neq 0$ and $\mathbb{Z}/3\mathbb{Z} \neq 0$. However, $\mathbb{Z}$ is not quasi-local and $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \dfrac{\mathbb{Z}/2\mathbb{Z}}{3(\mathbb{Z}/2\mathbb{Z})} = 0$. Also, if $R = \mathbb{Z}_{(2)}$, then $R \neq 0$ is local; however, $R/(2)_{(2)} \otimes_R \mathbb{Q} \cong \mathbb{Z}_{(2)}/2\mathbb{Q}_{(2)} \cong \mathbb{Q}/\mathbb{Q} = 0$ despite the fact that $R/(2)_{(2)} \neq 0$ and $\mathbb{Q} \neq 0$. This is okay because $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}_{(2)}-$module.

Note. Anything we've said about the functor $M \otimes_R -$ also holds for the functor $- \otimes_R M$ since they're naturally equivalent functors.

Definition 283. Let M be an $R-$module and define a functor $\mathrm{Hom}_R(M, -) : \mathbf{R-mod} \to \mathbf{R-mod}$ on objects as $N \longmapsto \mathrm{Hom}_R(M, N) = \{f : M \to N \mid f \text{ is an } R-\text{module homomorphism}\}$ and on morphisms as $(f : N_1 \to N_2) \longmapsto (f_* : \mathrm{Hom}_R(M, N_1) \to \mathrm{Hom}_R(M, N_2))$ where $f_*(g) = fg$.

Note. The functor $\mathrm{Hom}_R(M, -)$ is covariant, additive, and multiplicative.

[6] That result is due to Kunz in 1969.

4.6 Friday 20 April 2012

4.6.1 Tangent in Commutative Algebra

Lemma 284. *Let k be an infinite field and $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \setminus \{0\}$. then there exists some $(a_1, \ldots, a_n) \in k^n$ such that $f(a_1, \ldots, a_n) \neq 0$.*

Proof. We'll prove this using induction on n. When $n = 1$, then every nonzero polynomial, $f(x) \in k[x]$ has only finitely many roots. Since k is an infinite field, then there must be some $a \in k$ such that $f(a) = 0$. For the inductive step, let $n > 1$ and let $f \in k[x_1, \ldots, x_n]$ be such that $f \neq 0$. Note that we can write $f(x_1, \ldots, x_n) = f_r(x_1, \ldots, x_{n-1})x_n^r + f_{r-1}(x_1, \ldots, x_{n-1})x_n^{r-1} + \ldots + f_0(x_1, \ldots, x_{n-1})$ where $f_r \neq 0$. By induction, choose $(a_1, \ldots, a_{n-1}) \in k^{n-1}$ such that $f_r(a_1, \ldots, a_{n-1}) \neq 0$. Then, let $g(x_n) = f(a_1, \ldots, a_{n-1}, x_n) = f_r(a_1, \ldots, a_{n-1})x_n^r + \ldots + f_0(a_1, \ldots, a_{n-1})$. By the $n = 1$ case, we have that there is some $a_n \in k$ such that $f(a_1, \ldots, a_{n-1}, a_n) = g(a_n) \neq 0$. □

Note. Lemma 284 is false if k is a finite field. This is easily seen by considering $x^p - x$.

Proposition 285. *Let k be an infinite field and V a finite dimensional vector space. Then V is not the union of finitely many proper subspaces.*

Proof. Let $v_1, \ldots, v_n$ be a basis for V. Suppose that $V = W_1 \cup \ldots \cup W_t$ where W_i are proper subspaces of V. Without loss of generality, we can assume that $\dim W_i = n - 1$ for all i. Let $W \subseteq V$ be any $n - 1$ dimensional subspace with basis $\{u_1, \ldots, u_{n-1}\}$, then $u_i = \sum_{j=1}^n a_{i,j}v_j$ for some $a_{i,j} \in k$. Thus, $[a_{ij}]$ is an $n - 1$ by n matrix of rank $n - 1$. Let $v \in V$. Then $v = \sum_{i=1}^n c_i v_i$ for some $c_i \in k$. Then $v \in W$ if and only if

$$\operatorname{rank} \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n} \\ c_1 & c_2 & \ldots & c_n \end{bmatrix} = n - 1$$

which is true if and only if

$$\det \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n} \\ c_1 & c_2 & \ldots & c_n \end{bmatrix} = 0.$$

Let

$$f_W(x_1, \ldots, x_n) = \det \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n} \\ x_1 & x_2 & \ldots & x_n \end{bmatrix} \in k[x_1, \ldots, x_n]$$

and note that $f_W(c_1, \ldots, c_n) = 0$ if and only if $v \in W$. Also note that $f_W \neq 0$ since W is a proper subspace of V, so there is some $v' \in V \setminus W$. Now, let $f_i = f_{W_i}$ as constructed. Then set $f = \prod_{i=1}^t f_i \in k[x_1, \ldots, x_n]$ and $f \neq 0$ since each $f_i \neq 0$. As $|k| = \infty$, there is some $(c_1, \ldots, c_n) \in k^n$ such that $f(c_1, \ldots, c_n) \neq 0$. Thus, $f_i(c_1, \ldots, c_n) \neq 0$ for each i and so $v \notin W_i$ for all i. This is a contradiction since $V = W_1 \cup \ldots \cup W_t$ and so we must have that V cannot be written as the union of finitely many proper subspaces. □

Proposition 286. *Let $(R, \mathfrak{m})$ be a quasi-local ring and let M be a finitely generated $R-$module such that $R/\mathfrak{m}$ is an infinite field. Then M is not the union of finitely many proper subspaces.*

Proof. Suppose that $M = N_1 \cup \ldots \cup N_t$ where $N_1, \ldots, N_t$ are submodules of M. Then $M/\mathfrak{m}M = \dfrac{N_1 + \mathfrak{m}M}{\mathfrak{m}M} \cup \ldots \cup \dfrac{N_t + \mathfrak{m}M}{\mathfrak{m}M}$. Note that $M/\mathfrak{m}M$ is a finitely generated $R/\mathfrak{m}-$vector space. By the field case, $M/\mathfrak{m}M = \dfrac{N_i + \mathfrak{m}M}{\mathfrak{m}M}$ for some i. Then we have that $M = N_i + \mathfrak{m}M$ and so by Nakayama's Lemma (Lemma 231), we have that $M = N_i$. □

Remark 287. *The following is a useful way to force the quotient field to be infinite:* Suppose $(R, \mathfrak{m})$ is a quasi-local ring, and $R/\mathfrak{m}$ is a finite field. Consider the ring $S = R[x]_{\mathfrak{m}R[x]}$. Note that $\mathfrak{m}R[x] = \mathfrak{m}[x]$ is prime in $R[x]$ since

$R[x]/\mathfrak{m}R[x] \cong (R/\mathfrak{m})[x]$ is a domain since $R/\mathfrak{m}$ is a field. So S is a quasi-local ring. Let $\mathfrak{n} = \mathfrak{m}R[x]_{\mathfrak{m}R[x]}$ and note that $\mathfrak{n}$ is the unique maximal ideal of S. Then,

$$\frac{S}{\mathfrak{n}} = \frac{R[x]_{\mathfrak{m}R[x]}}{\mathfrak{m}R[x]_{\mathfrak{m}R[x]}} \cong \left(\frac{R[x]}{\mathfrak{m}R[x]}\right)_{\overline{\mathfrak{m}R[x]}} \cong (R/\mathfrak{m})[x]_{\overline{0}}$$

which is the field of fractions of $(R/\mathfrak{m})[x]$ and hence equal to $(R/\mathfrak{m})(x)$ which is an infinite field!

Proposition 288. *Let $\phi : R \to S$ be a ring homomorphism where S is a flat $R-$module (or in equivalent language, ϕ is a flat ring map). Let M be a flat $S-$module. Then M is a flat $R-$module.*

Proof. Let $0 \to A \to B$ be an injection of $R-$modules (that is, an exact sequence). Since S is flat as an $R-$module, then $0 \to A \otimes_R S \to B \otimes_R S$ is exact and now these are $S-$module homomorphisms. Since M is a flat $S-$module, then $0 \to (A \otimes_R S) \otimes_S M \to (B \otimes_R S) \otimes_S M$ is also exact. Using the associative property we proved for tensor products, then $0 \to A \otimes_R (S \otimes_S M) \to B \otimes_R (S \otimes_S M)$ is exact. Since $S \otimes_S M \cong M$, then we have that $0 \to A \otimes_R M \to B \otimes_R M$ is exact using Lemma 273 and hence M is a flat $R-$module since these are now $R-$module homomorphisms. □

Corollary 289. *If $\phi : R \to S$ and $\psi : S \to T$ are flat ring maps, then $\psi\phi : R \to T$ is also a flat ring map.*

Proof. This is done by taking $M = T$ from the previous proposition. □

Remark 290. The natural ring homomorphism $f : R \to S$ where R and S are as in Remark 287 is flat. Also, in the same context the maximal ideal of R extended to S is $mS = n$.

Proof. The map $\phi : R \to R[x]$ is flat since $R[x]$ is a free $R-$module. Also, $\psi : R[x] \to R[x]_{\mathfrak{m}R[x]}$ is flat because localization is always flat. Thus, $\psi\phi = f : R \to R[x]_{\mathfrak{m}R[x]}$ (which is the natural ring homomorphism) is a flat map by Corollary 289. □

Remark 291. Let $(R, \mathfrak{m})$ be quasi-local and M a finitely generated $R-$module. Consider $N = M \otimes_R S$ where $S = R[x]_{\mathfrak{m}R[x]}$. Then N is a finitely generated $S-$module and $|S/\mathfrak{n}| = \infty$ where $\mathfrak{n}$ is the maximal ideal of the quasi-local ring S.

Proposition 292. *In particular, in the case of the previous remark, we have $\lambda_R(M) = \lambda_S(N)$.*

Proof. We proceed by induction on $\lambda_R(M)$. When $\lambda_R(M) = 1$, then M is a simple module and so $M \cong R/\mathfrak{m}$. Thus, $N = M \otimes_R S \cong R/\mathfrak{m} \otimes_R S \cong S/\mathfrak{m}S \cong S/n$ which is a simple $S-$module, and so $\lambda_S(N) = 1$ as well. For the inductive step, assume that $\lambda_R(M) > 1$ and let $A \neq 0$ be a proper submodule of M. Then $0 \to A \to M \to M/A \to 0$ is an exact sequence of $R-$modules. By additivity of length on exact sequences (see Proposition 44), we have $\lambda_R(M) = \lambda_R(A) + \lambda_R(M/A)$. Note that S is flat by Remark 290. Thus, applying the functor $- \otimes_R S$ to the short exact sequence $0 \to A \to M \to M/A \to 0$ gives the short exact sequence

$$0 \to A \otimes_R S \to M \otimes_R S \to M/A \otimes_R S \to 0.$$

Since $\lambda_R(A), \lambda_R(M/A) < \lambda_R(M)$, then by our inductive hypothesis $\lambda_R(A) = \lambda_S(A \otimes_R S)$ and $\lambda_R(M/A) = \lambda_S(M/A \otimes_R S)$. Again using Proposition 44, we have that

$$\lambda_S(N) = \lambda_S(M \otimes_R S) = \lambda_S(A \otimes_R S) + \lambda_S(M/A \otimes_R S) = \lambda_R(A) + \lambda_R(M/A) = \lambda_R(M)$$

as desired. □

4.7 Monday 23 April 2012

4.7.1 Covariant Hom Functor

Recall. If M, N are $R-$modules, then $\mathrm{Hom}_R(M, N) := \{f : M \to N \mid f \text{ is an } R-\text{module homomorphism}\}$ is an $R-$module via $(rf)(m) = rf(m)$ and $(f_1 + f_2)(m) = f_1(m) + f_2(m)$.

Proposition 293. *Here are some useful isomorphisms:*

1. *For any $R-$module N, $\mathrm{Hom}_R(R, N) \cong N$ via the map $f \longmapsto f(1)$.*
2. *If I is an ideal of R and N is an $R-$module, then $\mathrm{Hom}_R(R/I, N) \cong (0 :_N I)$ via the map $f \longmapsto f(\overline{1})$. Note that $(0 :_N I) := \{u \in N \mid Iu = 0\}$.*
3. *If A, B, N are $R-$modules, then $\mathrm{Hom}_R(A \oplus B, N) \cong \mathrm{Hom}_R(A, N) \oplus \mathrm{Hom}_R(B, N)$ via the map $f \longmapsto (f|_A, f|_B)$.*

Proof. 1. Let $\phi : \mathrm{Hom}_R(R, N) \to N$ be defined by $\phi(f) = f(1)$. Then for any $f, g \in \mathrm{Hom}_R(R, N)$, we have $\phi(f + g) = (f + g)(1) = f(1) + g(1) = \phi(f) + \phi(g)$. Also, if $r \in R$, then $\phi(rf) = (rf)(1) = rf(1) = r\phi(f)$ and so ϕ is an $R-$module homomorphism. Next, suppose $\phi(f) = \phi(g)$, then $f(1) = g(1)$ and for any $r \in R$, $f(r) = f(r \cdot 1) = rf(1) = rg(1) = g(r \cdot 1) = g(r)$ and so $f = g$, which shows that ϕ is injective. Now, let $n \in N$. Then define an $R-$linear map $f : R \to N$ by $f(1) = n$. Then $\phi(f) = f(1) = n$ so that ϕ is surjective.

2. Let $\phi : \mathrm{Hom}_R(R/I, N) \to (0 :_N I)$ be defined by $\phi(f) = f(\overline{1})$. First we should check that the image of ϕ is contained in $(0 :_N I)$. So let $f \in \mathrm{Hom}_R(R/I, N)$. Then since f is an $R-$module homomorphism, $If(\overline{1}) = f(I\overline{1}) = f(\overline{0}) = 0$ so that $f(\overline{1}) \in (0 :_N I)$ as claimed. Next, we show that ϕ is an $R-$module homomorphism. Let $f, g \in \mathrm{Hom}_R(R/I, N)$. Then $\phi(f+g) = (f+g)(\overline{1}) = f(\overline{1})+g(\overline{1}) = \phi(f)+\phi(g)$. If additionally, $r \in R$, then $\phi(rf) = (rf)(\overline{1}) = rf(\overline{1}) = r\phi(f)$. Now, if $\phi(f) = \phi(g)$, then $f(\overline{1}) = g(\overline{1})$. The for any $r \in R$, we have that since f, g are $R-$module homomorphisms, $f(\overline{r}) = f(r\overline{1}) = rf(\overline{1}) = rg(\overline{1}) = g(r\overline{1}) = g(\overline{r})$ so that $f = g$ and ϕ is injective. Finally, if $n \in (0 :_N I)$, then $In = 0$. This means that we can define an $R-$module homomorphism $f : R \to N$ by $f(1) = n$ and that $I \subseteq \ker f$ and hence we have an induced $R-$module homomorphism $\widetilde{f} : R/I \to N$ where $\widetilde{f}(\overline{1}) = n$. Hence, $\phi(\widetilde{f}) = \widetilde{f}(\overline{1}) = n$ and so ϕ is surjective.
3. Let $\phi : \mathrm{Hom}_R(A \oplus B, N) \to \mathrm{Hom}_R(A, N) \oplus \mathrm{Hom}_R(B, N)$ be defined by $\phi(f) = (f|_A, f|_B)$. First, if $f, g \in \mathrm{Hom}_R(A \oplus B, N)$, then $\phi(f+g) = ((f+g)|_A, (f+g)|_B) = (f|_A + g|_A, f|_B + g|_B) = (f|_A, f|_B) + (g|_A, g|_B) = \phi(f) + \phi(g)$. If $r \in R$, then $\phi(rf) = ((rf)|_A, (rf)|_B) = (rf|_A, rf|_B) = r(f|_A, f|_B) = r\phi(f)$and so ϕ is an $R-$module homomorphism. Next, if $\phi(f) = \phi(g)$, then $f|_A = g|_A$ and $f|_B = g|_B$ so that for any $a + b \in A \oplus B$, we have $f(a + b) = f|_A(a) + f|_B(b) = g|_A(a) + g|_B(b) = g(a + b)$ so that ϕ is injective. Finally, if $(f, g) \in \mathrm{Hom}_R(A, N) \oplus \mathrm{Hom}_R(B, N)$, then define $f \oplus g : A \oplus B \to N$ by $(f \oplus g)(a \oplus b) = f(a) + g(b)$. Then $f \oplus g$ is an $R-$module homomorphism since f and g are, and hence $\phi(f \oplus g) = ((f \oplus g)|_A, (f \oplus g)|_B) = (f, g)$ and so ϕ is surjective.

□

Recall. Recall from Definition 283 that $\mathrm{Hom}_R(M, -)$ as a covariant, additive, multiplicative functor.

Remark 294. If S is an $R-$algebra and M is an $S-$module, then for any $R-$module, N, then $\mathrm{Hom}_R(M, N)$ has the structure of an $S-$module via $(sf)(m) := f(sm)$. Furthermore, if $g : N_1 \to N_2$ is an $R-$module homomorphism, then g_* as defined in Definition 283 is an $S-$module homomorphism. Thus, in this case, we have that $\mathrm{Hom}_R(M, -)$ is a functor from $\mathbf{R-mod}$ to $\mathbf{S-mod}$.

Proposition 295. *Let R be a commutative ring and M an $R-$module. Then the functor $\mathrm{Hom}_R(M, -)$ is left exact.*

Proof. Let

$$0 \longrightarrow A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C$$

be an exact sequence of $R-$modules. Then we must show that

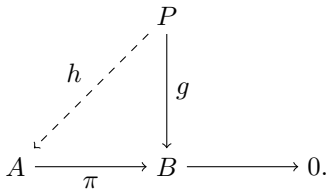
$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f_*} \mathrm{Hom}_R(M, B) \xrightarrow{g_*} \mathrm{Hom}_R(M, C)$$

is exact. We'll start by showing that f_* is injective. So suppose that $f_*(\alpha) = 0$ for some $\alpha \in \mathrm{Hom}_R(M, A)$. Then we have that $f\alpha = 0$. Since f is injective, then we must have that $\alpha = 0$ and hence f_* is injective as well. Next, since $\mathrm{Hom}_R(M, -)$ is a covariant functor and $gf = 0$ since the original sequence is exact, then $g_* \circ f_* = (gf)_* = 0_* = 0$. Thus, it only remains to show that $\ker(g_*) \subseteq \mathrm{image}(f_*)$. Let $\beta : M \to B$ be an $R-$module homomorphism such that $g_*(\beta) = 0$. Then by definition of g_*, we have $g\beta = 0$. This gives that $\mathrm{image}(\beta) \subseteq \ker(g) = \mathrm{image}(f)$ since the original sequence is exact. Define $h : M \to A$ by $h(m) := f^{-1}(\beta(m))$. This is well defined since $\beta(m) \in \mathrm{image}(f)$ for all $m \in M$ and f is injective. Then h is an $R-$module homomorphism since both f and β are. Also, $f_*(h) = fh = ff^{-1}\beta = \beta$ and so $\beta \in \mathrm{image}(f_*)$. Hence $\ker(g_*) = \mathrm{image}(f_*)$, which completes the proof. □

Example 296. This example shows that the functor $\mathrm{Hom}_R(M, -)$ need not preserve surjections. Consider the map $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ which is surjective. Applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ gives the map $\pi_* : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$. Since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \cong (0 :_{\mathbb{Z}} 2\mathbb{Z}) = 0$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ by Proposition 293, then π_* cannot be surjective.

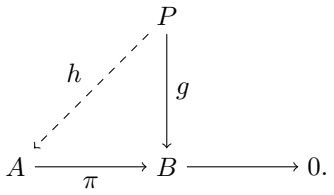
Proposition 297. *Let P be an $R-$module. Then P is projective if and only if $\mathrm{Hom}_R(P, -)$ is exact (which is equivalent by Proposition 295 to $\mathrm{Hom}_R(P, -)$ preserving surjections).*

Proof. ($\Rightarrow$) Let $\pi : A \to B$ be a surjection. We need to show that $\pi_* : \mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, B)$ is also surjective. Note that $\pi_*(\alpha) = \pi\alpha$. Let $g : P \to B$ be an $R-$module homomorphism, that is, $g \in \mathrm{Hom}_R(P, B)$. Then, as P is projective, there is a map $h : P \to A$ such that the following diagram commutes:



Equivalently, $\pi \circ h = \pi_*(h) = g$ and so $\pi_a st$ is surjective.

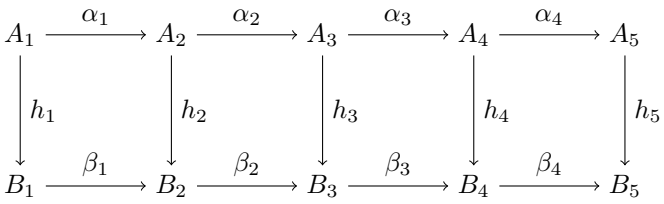
($\Leftarrow$) Let $\mathrm{Hom}_R(P, -)$ be exact, and suppose that $\pi : A \to B$ is a surjection. Then $\pi_* : \mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, B)$ is surjective as well. Then for any $g \in \mathrm{Hom}_R(P, B)$ there is a map $h \in \mathrm{Hom}_R(P, A)$ such that $\pi \circ h = \pi_*(h) = g$. Equivalently, given any diagram as below with exact row, there is a map $h : P \to A$ such that the diagram commutes.



□

4.7.2 5 Lemma

Lemma 298 (5-Lemma)**.** *Consider the following commutative diagram of $R-$modules, with exact rows.*



If h_1, h_2, h_4, h_5 are all isomorphisms, then h_3 is also an isomorphism.

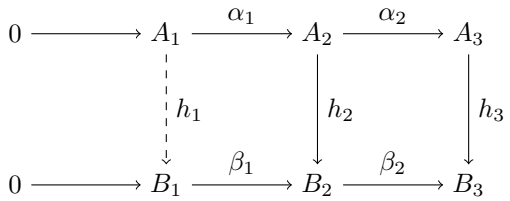
Proof. We'll first show that h_3 is surjective. Let $b_3 \in B_3$. Then there is some $a_4 \in A_4$ such that $h_4(a_4) = \beta_3(b_3)$. Notice that $h_5(\alpha_4(a_4)) = \beta_4(h_4(a_4)) = \beta_4(\beta_3(b_3)) = 0$ by commutativity of the diagram and since the bottom row is exact. Since h_5 is an isomorphism, then $\alpha_4(a_4) = 0$. Hence $a_4 \in \ker(\alpha_4) = \mathrm{image}(\alpha_3)$. Thus, there is some $a_3 \in A_3$ such that $\alpha_3(a_3) = a_4$. Notice that $\beta_3(b_3 - h_3(a_3)) = \beta_3(b_3) - \beta_3(h_3(a_3)) = \beta_3(b_3) - h_4(\alpha_3(a_3)) = \beta_3(b_3) - h_4(a_4) = \beta_3(b_3) - \beta_3(b_3) = 0$. Hence, $b_3 - h_3(a_3) \in \ker(\beta_3) = \mathrm{image}(\beta_2)$ and so there exists some $b_2 \in B_2$ such that $\beta_2(b_2) = b_3 - h_3(a_3)$. Since h_2 is an isomorphism, then there exists some $a_2 \in A_2$ such that $h_2(a_2) = b_2$. By commutativity of the diagram, we then have $h_3(\alpha_2(a_2)) = \beta_2(h_2(a_2)) = \beta_2(b_2) = b_3 - h_3(a_3)$. Hence, $b_3 = h_3(\alpha_2(a_2)) + h_3(a_3)$ and thus, $b_3 = h_3(\alpha_2(a_2) + a_3) \in \mathrm{image}(h_3)$ so that h_3 is surjective.

Next, we'll show that h_3 is injective. Let $h_3(a_3) = 0$. We wish to show that $a_3 = 0$. Note first that $0 = \beta_3(0) = \beta_3(h_3(a_3)) = h_4(\alpha_3(a_3))$ since the diagram commutes and β_3 is a homomorphism. As h_4 is an isomorphism, then $\alpha_3(a_3) = 0$. Thus, $a_3 \in \ker(\alpha_3) = \mathrm{image}(\alpha_2)$ since the top row is exact. So let $a_2 \in A_2$ be such that $\alpha_2(a_2) = a_3$. Then $\beta_2(h_2(a_2)) = h_3(\alpha_2(a_2)) = h_3(a_3) = 0$ since the diagram commutes. Hence, $h_2(a_2) \in \ker(\beta_2) = \mathrm{image}(\beta_1)$. So let $b_1 \in B_1$ be such that $\beta_1(b_1) = h_2(a_2)$. Since h_1 is an isomorphism, then there is some $a_1 \in A_1$ such that $h_1(a_1) = b_1$. By commutativity of the diagram we get that $h_2(\alpha_1(a_1)) = \beta_1(h_1(a_1)) = \beta_1(b_1) = h_2(a_2)$. Since h_2 is an isomorphism, then $\alpha_1(a_1) = a_2$. Also, since the top row is exact, then $0 = \alpha_2(\alpha_1(a_1)) = \alpha_2(a_2) = a_3$ and hence h_3 is injective. □

4.8 Wednesday 25 April 2012

4.8.1 5 Lemma Consequences

Proposition 299. *This is a special case of the 5-Lemma (Lemma 298). Consider the following commutative diagram with exact rows where h_2, h_3 are isomorphisms.*



Then there exists an isomorphism $h_1 : A_1 \to B_1$ such that the diagram commutes.

Proof. If there is a homomorphism $h_1 : A_1 \to B_1$ such that the diagram commutes, then using the 5-Lemma, since the larger diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & 0 & \longrightarrow & B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_4 \end{array}$$

commutes, both rows are exact, and h_2, h_3, h_4, h_5 are isomorphisms, then h_1 is an isomorphism. So let $a_1 \in A_1$ and note that $\beta_2(h_2(\alpha_1(a_1))) = h_3(\alpha_2(\alpha_1(a_1))) = h_3(0) = 0$. Thus, $\text{image}(h_2\alpha_1) \subseteq \ker(\beta_2) = \text{image}(\beta_1)$. Since β_1 is injective, then we can thus define $h_1 = \beta_1^{-1} h_2 \alpha_1$ and so by definition, the diagram commutes. □

Proposition 300. *Similarly, we have the following special case of the 5-Lemma (Lemma 298).*[7] *Consider the following commutative diagram with exact rows, where h_1, h_2 are isomorphisms.*

$$\begin{array}{ccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \vdots & & \\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \longrightarrow & 0 \end{array}$$

Then there exists an isomorphism $h_3 : A_3 \to B_3$ such that the diagram commutes.

Proof. Again, if there is a homomorphism $h_3 : A_3 \to B_3$ such that the diagram commutes, then using the 5-Lemma, since the larger diagram

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \longrightarrow & 0 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

commutes, both rows are exact, and h_1, h_2, h_4, h_5 are isomorphisms, then h_3 is an isomorphism. So choose any $a_3 \in A_3$. Since α_2 is surjective, there is some $a_2 \in A_2$ such that $\alpha_2(a_2) = a_3$. Suppose that $\alpha_2(a_2) = \alpha_2(a_2') = a_3$. Then, $\alpha_2(a_2 - a_2') = 0$ and so $a_2 - a_2' \in \ker(\alpha_2) = \text{image}(\alpha_1)$ and there exists some $a_1 \in A_1$ such that $\alpha_1(a_1) = a_2 - a_2'$. Since the bottom row is exact, and since the original diagram commutes, we have $0 = \beta_2(\beta_1(h_1(a_1))) = \beta_2(h_2(\alpha_1(a_1))) = \beta_2(h_2(a_2 - a_2')) = \beta_2(h_2(a_2)) - \beta_2(h_2(a_2'))$ and so $\beta_2 h_2$ is constant on $\alpha_2^{-1}(a_3)$. Hence, the map $h_3 : A_3 \to B_3$ defined by $h_3(a_3) = \beta_2(h_2(a_2))$ for any $a_2 \in A_2$ such that $\alpha_2(a_2) = a_3$ is well defined, and a homomorphism. The diagram commutes since $h_3(\alpha_2(a_2)) = \beta_2(h_2(a_2))$ by definition of h_3. □

4.8.2 Contravariant Hom Functor

Definition 301. Let N be an $R-$module, and $g : M_1 \to M_2$ an $R-$module homomorphism. Then, define $g^* : \text{Hom}_R(M_2, N) \to \text{Hom}_R(M_1, N)$ via $\alpha \longmapsto \alpha g$. Then g^* is an $R-$module homomorphism. We can thus define a functor $\text{Hom}_R(-, N) : \mathbf{R-mod} \to \mathbf{R-mod}$ on objects by sending M to $\text{Hom}_R(M, N)$ and on morphisms $g : M_1 \to M_2$ to g^*.

Note. The functor $\text{Hom}_R(-, N)$ is contravariant, additive, and multiplicative. Also, as before, if N is also an $S-$module, for some $R-$algebra, S, then $\text{Hom}_R(-, N)$ can be thought of as a functor from $\mathbf{R-mod}$ to $\mathbf{S-mod}$ since for $f \in \text{Hom}_R(M, N)$ and $s \in S$, we have $(sf)(m) = sf(m)$.

Proposition 302. *If N is an $R-$module, then $\text{Hom}_R(-, N)$ is left exact. That is, given an exact sequence $A \to B \to C \to 0$, the sequence $0 \to \text{Hom}_R(C, N) \to \text{Hom}_R(B, N) \to \text{Hom}_R(A, N)$ is also exact with the appropriate maps.*

Proof. Let the sequence

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be exact. Then we must show that the sequence

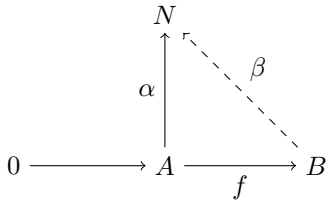
[7] He alluded to this in class, but didn't even bother to state it.

$$0 \longrightarrow \mathrm{Hom}_R(C,N) \xrightarrow{g^*} \mathrm{Hom}_R(B,N) \xrightarrow{f^*} \mathrm{Hom}_R(A,N)$$

is also exact. We'll first show that g^* is injective. So let $\gamma \in \mathrm{Hom}_R(C,N)$ and suppose that $g^*(\gamma) = 0$. Then $\alpha \circ g = 0$. Since g is surjective, this then gives that $\alpha = 0$. Next, since the original sequence is exact, then $gf = 0$ and so applying the contravariant functor $\mathrm{Hom}_R(-,N)$ gives that $f^* \circ g^* = (gf)^* = 0^* = 0$. It thus only remains to show that $\ker(g^*) \subseteq \text{image}(f^*)$. So let $\beta \in \mathrm{Hom}_R(B,N)$ such that $\beta f = f^*(\beta) = 0$. Suppose that $g(b) = g(b')$, then $b - b' \in \ker(g) = \text{image}(f)$ by the exactness of the original sequence and so there exists some $a \in A$ such that $f(a) = b - b'$. Thus, $0 = \beta(f(a)) = \beta(b - b') = \beta(b) - \beta(b')$ and so β is constant on $g^{-1}(c)$. Hence, there is some $\gamma \in \mathrm{Hom}_R(C,N)$ such that $\gamma = \beta g^{-1}$. Since $g^*(\gamma) = g^*(\beta g^{-1}) = \beta g^{-1} g = \beta$, then $\beta \in \text{image}(g^*)$ and hence $\ker(f^*) \subseteq \text{image}(g^*)$ as required. □

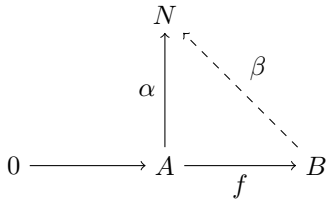
Proposition 303. *The functor* $\mathrm{Hom}_R(-,N)$ *is exact if and only if* N *is injective. Note here that we know by Proposition 302* $\mathrm{Hom}_R(-,N)$ *is exact if and only if it takes injections to surjections.*

Proof. ($\Rightarrow$) Let $f : A \to B$ be an injection. Since $f^* : \mathrm{Hom}_R(B,N) \to \mathrm{Hom}_R(A,N)$ is surjective, then for any $\alpha \in \mathrm{Hom}_R(A,N)$ there is some $\beta \in \mathrm{Hom}_R(B,N)$ such that $\beta f = f^*(\beta) = \alpha$. That is, in the diagram



with exact row there exists an $R-$module homomorphism $\beta : B \to N$ such that the diagram commutes. Hence, by definition, N is injective.

($\Leftarrow$) Now suppose that N is an injective $R-$module. Then suppose $f : A \to B$ is an injective $R-$module homomorphism, and let $\alpha \in \mathrm{Hom}_R(A,N)$. Then in the commutative diagram



with exact row, there exists an $R-$module homomorphism β such that the diagram commutes. Hence, $f^*(\beta) = \beta f = \alpha$ and so f^* is surjective as desired. □

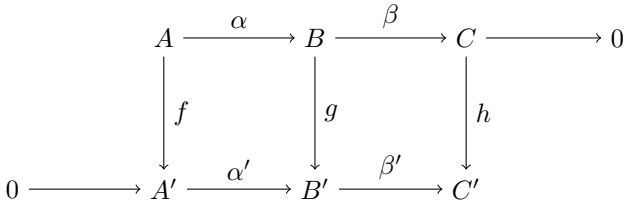
Definition 304. An $R-$module is called *finitely presented* if there exists an exact sequence of the form

$$R^m \to R^n \to M \to 0.$$

That is, both M and $\ker(R^n \to M)$ are finitely generated.

Definition 305. Let $f : A \to B$ be an $R-$module homomorphism. Then $\mathrm{coker}(f) = B/f(A)$ is called the *cokernel* of f.

Lemma 306 (Snake Lemma[8]). *Let*



be a commutative diagram of $R-$*modules with exact rows. Then there is a map* $\delta : \ker(h) \to \mathrm{coker}(f)$ *such that the sequence*

[8]This wasn't even stated in class, but is super useful in commutative algebra and is used to prove things that also weren't shown in class.

$$\ker(f) \xrightarrow{\widehat{\alpha}} \ker(g) \xrightarrow{\widehat{\beta}} \ker(h) \xrightarrow{\delta} \operatorname{coker}(f) \xrightarrow{\widehat{\alpha'}} \operatorname{coker}(g) \xrightarrow{\widehat{\beta'}} \operatorname{coker}(h)$$

is exact.

Proof. First, note that $\ker(f) \subseteq A$, $\ker(g) \subseteq B$, and $\ker(h) \subseteq C$. Also, if $a \in \ker(f)$, then $g\alpha(a) = \alpha' f(a) = \alpha'(0) = 0$ by commutativity, and so $\alpha(a) \in \ker(g)$. Thus, we define $\widehat{\alpha}$ to be α restricted to $\ker(f)$. Similarly, for any $b \in \ker(g)$, then $\beta(b) \in \ker(h)$ and so we define $\widehat{\beta}$ to be β restricted to $\ker(g)$. Next, if $a' + f(A) \in \operatorname{coker}(f)$, then $\alpha'(a') + g(B) \in \operatorname{coker}(g)$, and for $b' + g(B) \in \operatorname{coker}(g)$, then $\beta'(b') + h(C) \in \operatorname{coker}(h)$, and we define $\widehat{\alpha'}(a' + f(A)) = \alpha'(a') + g(B)$ and $\widehat{\beta'}(b' + g(B)) = \beta'(b') + h(C)$. We must show these are well defined however, so let $a_1' + f(A) = a_2' + f(A)$. Then there is some $a \in A$ such that $a_1' = a_2' + f(a)$. Then,

$$\begin{aligned}
\widehat{\alpha'}(a_1' + f(A)) &= \alpha'(a_1') + g(B) \\
&= \alpha'(a_2' + f(a)) + g(B) \\
&= \alpha'(a_2') + \alpha'(f(a)) + g(B) \\
&= \alpha'(a_2') + g(\alpha(a)) + g(B) \\
&= \alpha'(a_2') + g(B) \\
&= \widehat{\alpha'}(a_2 + f(A))
\end{aligned}$$

due to the commutativity of the diagram, the fact that α' is an $R-$module homomorphism and since $g(\alpha(a)) \in g(B)$. The proof that $\widehat{\beta'}$ is well defined is the same as that for $\widehat{\alpha'}$, mutatis mutandis.

Next, we'll construct the map $\delta : \ker(h) \to \operatorname{coker}(f)$, so let $c \in \ker(h)$. Then there is some $b \in B$ such that $\beta(b) = c$ since β is surjective. By commutativity of the diagram and since $c \in \ker(h)$, we have that $\beta' g(b) = h\beta(b) = h(c) = 0$. Thus, $g(b) \in \ker(\beta') = \operatorname{image}(\alpha')$ since the bottom row is exact. We hence have that there is some $a' \in A'$ such that $\alpha'(a') = g(b)$. Set $\delta(c) = a' + f(A)$ so that $\delta(c) \in \operatorname{coker}(f)$ as desired.

We need to show that using this definition, δ is a well defined $R-$module homomorphism. Since α' is injective, then the choice of a' given the element b is unique, so to show the map is well defined, we only need to show it is independent of the choice of b. So suppose that $\beta(b) = \beta(\widetilde{b}) = c$. Then let $a', \widetilde{a'} \in A'$ be the unique elements such that $\alpha'(a') = g(b)$ and $\alpha'(\widetilde{a'}) = g(\widetilde{b})$. We need to show that $a' + \operatorname{image}(f) = \widetilde{a'} + \operatorname{image}(f)$. Since β is an $R-$module, then $\beta\left(b - \widetilde{b}\right) = \beta(b) - \beta\left(\widetilde{b}\right) = c - c = 0$. Since the top row is exact, then there is some $a \in A$ such that $\alpha(a) = b - \widetilde{b}$. Since the diagram commutes, and since g, α' are $R-$module homomorphisms, we then have $\alpha'(f(a)) = g(\alpha(a)) = g\left(b - \widetilde{b}\right) = g(b) - g\left(\widetilde{b}\right) = \alpha'(a') - \alpha'\left(\widetilde{a'}\right) = \alpha'\left(a' - \widetilde{a'}\right)$. Since α' is injective, then we have that $f(a) = a' - \widetilde{a'}$ and so $a' = \widetilde{a'} + f(a)$. Thus $a' + \operatorname{image}(f) = \widetilde{a'} + \operatorname{image}(f)$ and so δ is well defined.

To show δ is an $R-$module homomorphism, let $c_1, c_2 \in \ker(h)$ and $r \in R$. Then, we have $a_1', a_2' \in A'$ such that $\alpha'(a_1') = g(b_1)$ and $\alpha'(a_2') = b_2$ where $\beta(b_1) = c_1$ and $\beta(b_2) = c_2$. We thus have that $rc_1 + c_2 \in \ker(h)$ since $\ker(h)$ is an $R-$module and that $\beta(rb_1 + b_2) = r\beta(b_1) + \beta(b_2) = rc_1 + c_2$ since β is an $R-$module homomorphism. Also, $g(rb_1 + b_2) = rg(b_1) + g(b_2) = r\alpha'(a_1') + \alpha'(a_2') = \alpha'(ra_1' + a_2')$. Thus, $\delta(rc_1 + c_2) = ra_1' + a_2' + f(A) = r(a_1' + f(A)) + (a_2' + f(A)) = r\delta(c_1) + \delta(c_2)$ so that δ is an $R-$module homomorphism.

It remains to show that the sequence is exact. So let $a \in \ker(f)$. Then, $\widehat{\beta}(\widehat{\alpha}(a)) = \beta(\alpha(a)) = 0$ since the original diagram has exact rows. Now, if $b \in \ker(\widehat{\beta})$, then $\beta(b) = 0$ and so by exactness of the original diagram, there is some $a \in A$ such that $\alpha(a) = b$. If $a \in \ker(f)$, then we'll have that $\ker\widehat{\beta} = \operatorname{image}\widehat{\alpha}$. By commutativity of the diagram, we have that $\alpha'(f(a)) = g(\alpha(a)) = g(b) = 0$. Since α' is injective, then $f(a) = 0$ and so $a \in \ker(f)$ as desired.

Let $b \in \ker(g)$. Then, $\delta(\widehat{\beta}(b)) = \delta(\beta(b)) = a' + f(A)$ where $a' \in A$ is such that $\alpha'(a') = g(b)$. Also, $g(b) = 0$ since $b \in \ker(g)$, and so $\alpha'(a') = 0$. Since α' is injective, then $a' = 0$, and so $\delta(\widehat{\beta}(b)) = 0 + f(A) = 0 \in \operatorname{coker}(f)$. Next, let $c \in \ker(\delta)$. Then there is some $b \in B$ such that $\beta(b) = c$ and there is some $a' \in A'$ such that $\alpha'(a') = g(b)$. Since $\delta(c) = 0$, then $a' + f(A) = f(A)$ and so $a' \in f(A)$. Let $a \in A$ be chosen so that $f(a) = a'$. Then consider $b - \alpha(a)$. We have $\beta(b - \alpha(a)) = \beta(b) - \beta\alpha(a) = \beta(b)$ by the exactness of the original diagram. Also, $g(b - \alpha(a)) = g(b) - g(\alpha(a)) = g(b) - \alpha' f(a) = g(b) - \alpha'(a') = 0$ and so $c \in \operatorname{image}(\widehat{\beta})$ as desired.

Let $c \in \ker(h)$. Then, $\delta(c) = a' + f(A)$ where $\alpha'(a') = g(b)$ and $\beta(b) = c$. So $\alpha'(\delta(c)) = \widehat{\alpha'}(a' + f(A)) = \alpha'(a') + g(B) = g(b) + g(B) = 0 + g(B)$ and so $\operatorname{image}(\delta) \subseteq \ker\left(\widehat{\alpha'}\right)$. Net, let $a' + f(A) \in \ker\left(\widehat{\alpha'}\right)$. Then we have $\alpha'(a') + g(B) = 0 \in \operatorname{coker}(g)$ and so $\alpha'(a') \in g(B)$. Then let $b \in B$ be such that $g(b) = \alpha'(a')$. Then by definition, $\delta(\beta(b)) = a' + f(A)$ and so $\ker\left(\widehat{\alpha'}\right) = \operatorname{image}(\delta)$.

Finally, let $a' + f(A) \in \operatorname{coker}(f)$. Then, $\widehat{\beta'}(\widehat{\alpha'}(a' + f(A))) = \widehat{\beta'}(\alpha'(a') + g(B)) = \beta'(\alpha'(a')) + h(C) = 0 + h(C)$ since the original diagram had exact rows. Conversely, let $b' + g(B) \in \ker\left(\widehat{\beta'}\right)$. Then $0 = \widehat{\beta'}(b' + g(B)) = \beta'(b') + h(C)$,

and so $\beta'(b') \in h(C)$. Thus, there is some $c \in C$ such that $h(c) = \beta'(b')$. By exactness of the original top row, we have that there is some $b \in B$ such that $\beta(b) = c$. Then by commutativity of the original diagram, we have that $\beta'(g(b)) = h(\beta(b)) = h(c) = \beta'(b')$, and so $\beta'(b' - g(b)) = 0$. Hence, by exactness of the original bottom row, there is some $a' \in A'$ such that $\alpha'(a') = b - g(b)$. Hence, $\widehat{\alpha'}(a' + f(A)) = \alpha'(a') + g(B) = b' - g(b) + g(B) = b' + g(B)$ as desired. □

Lemma 307. *Suppose M is a finitely presented $R-$module and let*

$$0 \to K \to N \to M \to 0$$

be a short exact sequence where N is finitely generated. Then K is also finitely generated.[9]

Proof. Let

$$0 \longrightarrow K \xrightarrow{f} N \xrightarrow{g} M \longrightarrow 0$$

be an exact sequence of $R-$modules where M is finitely presented and N is finitely generated. Then there is an exact sequence of the form

$$R^s \xrightarrow{\phi} R^t \xrightarrow{\psi} M \longrightarrow 0$$

for some $m, n \in \mathbb{N}_1$. Let $e_1, \ldots, e_t$ be an $R-$module basis for R^t. For each i, then $\psi(e_i) \in M$. Since g is surjective, then there exist elements $n_1, \ldots, n_t \in N$ such that $g(n_i) = \psi(e_i)$ for each i. Define an $R-$module homomorphism $\alpha : R^t \to N$ by $\alpha(e_i) = n_i$. This gives the commutative diagram

$$\begin{array}{ccccccccc} & & R^s & \xrightarrow{\phi} & R^t & \xrightarrow{\psi} & M & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & K & \xrightarrow{f} & N & \xrightarrow{g} & M & \longrightarrow & 0 \end{array}$$

with exact rows. The left square commutes since if $(r_1, \ldots, r_t) \in R^t$, then

$$\begin{aligned} \psi(r_1, \ldots, r_t) &= r_1\psi(e_1) + \ldots + r_t\psi(e_t) \\ &= r_1 g(n_1) + \ldots + r_t g(n_t) \\ &= r_1 g(\alpha(e_1)) + \ldots + r_t g(\alpha(e_t)) \\ &= g\alpha((r_1, \ldots, r_t)) \end{aligned}$$

as desired. If we can define a homomorphism $\beta : R^s \to K$ such that the left square commutes, then we'll be able to apply the Snake Lemma (Lemma 306). Let $\epsilon_1, \ldots, \epsilon_s$ be a basis for R^s. For each i, we have that $g\alpha\psi(\epsilon_i) = \phi\psi(\epsilon_i) = 0$ since the top row is exact and by commutativity of the diagram. Hence, $\alpha\phi(\epsilon_i) \in \ker(g) = \text{image}(f)$ for all i. Since f is injective there is thus a unique $k_i \in K$ such that $f(k_i) = \alpha\phi(\epsilon_i)$. We then define the $R-$module homomorphism $\beta : R^s \to K$ by $\beta(e_i) = k_i$. Then the diagram commutes by definition, and so by the Snake Lemma, the following sequence is exact:

$$\ker(\beta) \to \ker(\alpha) \to 0 \to \text{coker}(\beta) \to \text{coker}(\alpha) \to 0$$

since the map 1_M is an isomorphism on M and so $\ker(1_M) = 0$ and $\text{coker}(1_M) = M/M = 0$. Hence,

$$K/\beta(R^s) = \text{coker}(\beta) \cong \text{coker}(\alpha) = N/\alpha(R^t).$$

Since N is finitely generated, then $N/\alpha(R^t)$ is finitely generated, and so $K/\beta(R^s)$ is also finitely generated. Since R^s is also finitely generated, then $\beta(R^s)$ is finitely generated. Thus, K is finitely generated. □

Remark 308. If R is Noetherian, then M is finitely presented if and only if M is finitely generated.

Proof. ($\Rightarrow$) If M is finitely presented, then M is automatically finitely generated.

($\Leftarrow$) Let $f : R^n \to M$ be surjective. Such a surjection exists since M is finitely generated. Let $K = \ker(f)$. Then $K \subseteq R^n$ is a submodule of R^n which is a Noetherian $R-$module, and so K is also finitely generated. Thus, M is finitely presented. □

[9] This was not proved in class, it was only indicated that the Snake Lemma would be useful.

Remark 309. Let I be an ideal of R. Then R/I is finitely presented if and only if I is finitely generated.

Proof. Since I is an ideal of R, then the sequence $0 \to I \to R \to R/I \to 0$ is exact.

($\Rightarrow$) If R/I is finitely presented, then since R is clearly finitely generated (as an $R-$module), we have that I is finitely generated by Lemma 307.

($\Leftarrow$) If I is finitely generated, then since $I = \ker(\pi)$ where π is the canonical quotient map, we have that R/I is finitely presented by definition. □

Proposition 310. *Let S be a flat $R-$algebra, let M, N be $R-$modules, and assume that M is finitely presented. Then $\mathrm{Hom}_R(M,N) \otimes_R S \cong \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$ via the map $f \otimes s \longmapsto f \otimes s$ where $f \otimes s$ on the right is the map $f \otimes s : M \otimes_R S \to N \otimes_R S$ given by $m \otimes s' \longmapsto f(m) \otimes ss'$.*

Proof. We first do the case when $M = R^n$. Then, using parts 1 and 3 of Proposition 293, we have $\mathrm{Hom}_R(M,N) = \mathrm{Hom}_R(R^n, N) \cong \bigoplus_{i=1}^{n} \mathrm{Hom}_R(R,N) \cong \bigoplus_{i=1}^{n} N = N^n$. Hence,

$$\begin{aligned}
\mathrm{Hom}_R(M,N) \otimes_R S &= \mathrm{Hom}_R(R^n, N) \otimes_R S \\
&\cong N^n \otimes_R S \\
&\cong (N \otimes_R S)^n \\
&\cong (\mathrm{Hom}_S(S, N \otimes_R S))^n \\
&\cong \mathrm{Hom}_S(S^n, N \otimes_R S) \\
&\cong \mathrm{Hom}_S(R^n \otimes_R S, N \otimes_R S) \\
&\cong \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S).
\end{aligned}$$

Chasing through the isomorphisms, we have the map as given in the statement.[10]

Now, we'll do the general case. As M is finitely presented, then there is an exact sequence

$$R^m \to R^n \to M \to 0. \tag{4.1}$$

Applying $- \otimes_R S$ to sequence (4.1) gives that the sequence

$$R^m \otimes_R S \to R^n \otimes_R S \to M \otimes_R S \to 0 \tag{4.2}$$

is also exact. Then applying the functor $\mathrm{Hom}_S(-, N \otimes_R S)$ to sequence (4.2) gives that the sequence

$$0 \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S) \to \mathrm{Hom}_S(R^n \otimes_R S, N \otimes_R S) \to \mathrm{Hom}_S(R^m \otimes_R S, N \otimes_R S) \tag{4.3}$$

is exact. Starting again with sequence (4.1), and applying the functor $\mathrm{Hom}_R(-, N)$ gives that the sequence

$$0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(R^n, N) \to \mathrm{Hom}_R(R^m, N) \tag{4.4}$$

is exact. Since S is flat, then the functor $- \otimes_R S$ is exact, and so applying it to sequence (4.4) gives that the sequence

$$0 \to \mathrm{Hom}_R(M,N) \otimes_R S \to \mathrm{Hom}_R(R^n, N) \otimes_R S \to \mathrm{Hom}_R(R^m, N) \otimes_R S \tag{4.5}$$

is also exact. We then have the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(M,N) \otimes_R S & \longrightarrow & \mathrm{Hom}_R(R^n, N) \otimes_R S & \longrightarrow & \mathrm{Hom}_R(R^m, N) \otimes_R S \\
 & & \downarrow h_1 & & \downarrow h_2 & & \downarrow h_3 \\
0 & \longrightarrow & \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(R^n \otimes_R S, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(R^m \otimes_R S, N \otimes_R S)
\end{array}$$

with exact rows by sequences (4.5) and (4.3), and isomorphisms h_2, h_3 by the first case. By Proposition 299, then there exists an isomorphism $h_1 : \mathrm{Hom}_R(M,N) \otimes_R S \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$ such that the entire diagram commutes. In particular, we have that $\mathrm{Hom}_R(M,N) \otimes_R S \cong \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$ as desired. □

Corollary 311. *If W is a multiplicatively closed subset of R, M is a finitely presented $R-$module, and N is any $R-$module, then $\mathrm{Hom}_R(M,N)_W \cong \mathrm{Hom}_{R_W}(M_W, N_W)$.*

[10] I got a bit lost in checking it, because of poorly named maps, but I'm sure it works.

Proof. Note that R_W is a flat $R-$module by Proposition 276. Hence, by Proposition 310 and part 3 of Proposition 254, we have that $\mathrm{Hom}_R(M,N)_W \cong \mathrm{Hom}_R(M,N)\otimes_R R_W \cong \mathrm{Hom}_{R_W}(M\otimes_R R_W, N\otimes_R R_W) \cong \mathrm{Hom}_{R_W}(M_W, N_W)$ as desired. □

Theorem 312. *Let M be a finitely presented $R-$module. Then the following are equivalent:*

1. *M is projective,*
2. *M_P is a free R_P-module for every $P \in \mathrm{Spec}(R)$, and*
3. *M_m is a free R_m-module for every maximal ideal m of R.*

Proof. $(1 \Rightarrow 2)$ By Proposition 243, then every finitely generated projective R_P-module is free. Since M is finitely presented, then M is also finitely generated, and by the last part of Remark 223, we know that M_P is a finitely generated R_P-module. By Corollary 229, then M_P is a projective R_P-module as well. Hence, M_P is a free R_P-module for every $P \in \mathrm{Spec}(R)$.

$(2 \Rightarrow 3)$ This is trivial since every maximal ideal is prime.

$(3 \Rightarrow 1)$ Note that it is enough by Proposition 297 to show that $\mathrm{Hom}_R(M,-)$ is exact, or equivalently, that it preserves surjections. So let $f : A \to B$ be a surjection of $R-$modules. We then need to show that $f_* : \mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B)$ is surjective as well. Let $C = \mathrm{coker}(f_*) = \mathrm{Hom}_R(M,B)/\,\mathrm{image}(f_*)$. Then the sequence

$$\mathrm{Hom}_R(M,A) \xrightarrow{f_*} \mathrm{Hom}_R(M,B) \longrightarrow C \longrightarrow 0$$

is exact. We need to show that $C = 0$. Let m be an arbitrary maximal ideal of R, and localizing the sequence at m gives that

$$\mathrm{Hom}_R(M,A)_m \xrightarrow{\frac{f_*}{1}} \mathrm{Hom}_R(M,B)_m \longrightarrow C_m \longrightarrow 0$$

is exact as well. Starting again with $f : A \to B$, localizing at m gives that

$$A_m \xrightarrow{\frac{f}{1}} B_m \longrightarrow 0$$

is exact. Applying the functor $\mathrm{Hom}_{R_m}(M_m,-)$ to this sequence gives that

$$\mathrm{Hom}_{R_m}(M_m,A_m) \xrightarrow{\frac{f}{1}} \mathrm{Hom}_{R_m}(M_m,B_m) \longrightarrow 0$$

is exact as well. We thus have the following commutative diagram

$$\begin{array}{ccccccc}
\mathrm{Hom}_R(M,A)_m & \xrightarrow{\alpha_1} & \mathrm{Hom}_R(M,B)_m & \xrightarrow{\alpha_2} & C_m & \longrightarrow & 0 \\
\downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \vdots{\scriptstyle h_3} & & \\
\mathrm{Hom}_{R_m}(M_m,A_m) & \xrightarrow{\beta_1} & \mathrm{Hom}_{R_m}(M_m,B_m) & \xrightarrow{\beta_2} & 0 & \longrightarrow & 0
\end{array}$$

with exact rows as shown above, and homomorphisms h_1, h_2 by Corollary 311. Thus, by Proposition 300, we have that $C_m \cong 0$. Then by Proposition 225, we have that $C = 0$ which completes the proof. □

4.9 Friday 27 April 2012

4.9.1 Adjointness of Hom and Tensor

Theorem 313 (Adjointnes of Tensor Product and Hom)**.** *Let S be an $R-$algebra, A, B $S-$modules, and C an $R-$module. Then there exists a natural isomorphism $\phi : \mathrm{Hom}_R(A\otimes_S B, C) \to \mathrm{Hom}_S(A, \mathrm{Hom}_R(B,C))$ given by $(f : A\otimes_S B \to C) \longmapsto (\phi(f) : A \to \mathrm{Hom}_R(B,C))$ where $\phi(f)(a) : B \to C$ is given by $b \longmapsto f(a\otimes b)$.*[11]

Theorem 314. *Another version of the Hom-Tensor Adjointness is: If A is an $R-$module, and B, C are $S-$modules, then there is an isomorphism $\mathrm{Hom}_S(A\otimes_R B, C) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C))$ as abelian groups.*[12]

[11] Tom didn't prove this in class, but he said it was an exercise. I'm going to prove the second version, but not this one. I'm pretty sure this version has a similar proof.

[12] Tom didn't explicitly state it, but I'm pretty sure we need here that S is an $R-$algebra.

Proof. The map $\phi : \mathrm{Hom}_S(A \otimes_R B, C) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$ is defined for each $f : A \otimes_R B \to C$ by $(\phi(f(a)))(b) = f(a \otimes b)$. We first must check that $\phi(f(a)) : B \to C$ is an $S-$module homomorphism. So let $b_1, b_2 \in B$ and $s \in S$. Then

$$\begin{aligned} \phi(f(a))(b_1 + sb_2) &= f(a \otimes (b_1 + sb_2)) \\ &= f(a \otimes b_1 + a \otimes sb_2) \\ &= f(a \otimes b_1) + f(a \otimes sb_2) \\ &= f(a \otimes b_1) + sf(a \otimes b_2) \\ &= \phi(f(a))(b_1) + s\phi(f(a))(b_2) \end{aligned}$$

since f is an $S-$module homomorphism and tensor products are linear. Next, we must check that $\phi(f) : A \to \mathrm{Hom}_S(B, C)$ is an $R-$module homomorphism. So let $a_1, a_2 \in A$, $r \in R$, and $b \in B$. Then,

$$\begin{aligned} \phi(f(a_1 + ra_2))(b) &= f((a_1 + ra_2) \otimes b) \\ &= f(a_1 \otimes b + ra_2 \otimes b) \\ &= f(a_1 \otimes b) + rf(a_2 \otimes b) \\ &= \phi(f(a_1))(b) + r\phi(f(a_2))(b) \end{aligned}$$

again since f is an $S-$module homomorphism (and $r \in R \subseteq S$) and tensor products are linear. Next, we must check that ϕ is a group homomorphism. So let $f, g \in \mathrm{Hom}_S(A \otimes_R B, C)$. We must show that $\phi(f + g) = \phi(f) + \phi(g)$. So let $a \in A$, and $b \in B$, then

$$\begin{aligned} \phi(f + g)(a)(b) &= (f + g)(a \otimes b) \\ &= f(a \otimes b) + g(a \otimes b) \\ &= \phi(f)(a)(b) + \phi(g)(a)(b) \end{aligned}$$

by definition of ϕ and by definition of a sum of maps, and so ϕ is a group homomorphism.
Next, we define a map $\psi : \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \to \mathrm{Hom}_S(A \otimes_R B, C)$ by $\psi(f) : A \otimes_R B \to C$ by $\psi(f)(a \otimes b) = f(a)(b)$. In order to do this we should first define $\widetilde{\psi(f)} : A \times B \to C$ as $\widetilde{\psi(f)}(a, b) = f(a)(b)$. Then, it is easy to check that $\widetilde{\psi(f)}$ is an $R-$bilinear map, and so it induces the map $\psi(f)$ we want.[13] We must however check that ψ is a group homomorphism. Let $f, g \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$, $a \in A$, and $b \in B$. Then

$$\begin{aligned} \psi(f + g)(a)(b) &= (f + g)(a \otimes b) \\ &= f(a \otimes b) + g(a \otimes b) \\ &= \psi(f)(a)(b) + \psi(f)(a)(b) \end{aligned}$$

by definition of ψ and by definition of a sum of maps, and so ψ is a group homomorphism. It only remains then to show that ψ and ϕ are inverses. Let $f \in \mathrm{Hom}_S(A \otimes_B, C)$, $a \in A$ and $b \in B$. Then, $\psi(\phi(f)) : A \otimes_R B \to C$ and is given by $\psi(\phi(f))(a \otimes b) = \phi(f)(a)(b) = f(a \otimes b)$ by definition of ψ and then ϕ respectively. Similarly, if $g \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$, $a \in A$ and $b \in$B, then $\phi(\psi(g)) : A \to \mathrm{Hom}_S(B, C)$ and is given by $\phi(\psi(g))(a)(b) = \psi(g)(a \otimes b) = g(a)(b)$ by definition of ϕ and then ψ respectively. Thus, ϕ and ψ are inverses and this gives the isomorphism as desired. □

Proposition 315. *Let S be an $R-$algebra, and I and injective $R-$module. Then* $\mathrm{Hom}_R(S, I)$ *is an injective $S-$module.*

Proof. It is enough to show that $\mathrm{Hom}_S(-, \mathrm{Hom}_R(S, I))$ is exact. It is always left exact, so it is exact if and only if it takes surjections to injections. So let $A \to B \to 0$ be an exact sequence of $S-$modules. Applying the functor in question gives the map $\mathrm{Hom}_S(B, \mathrm{Hom}_R(S, I)) \to \mathrm{Hom}_S(A, \mathrm{Hom}_R(S, I))$, and we want to show that it is injective. By the adjointness of tensor products and Hom (Theorem 313), we have the following commutative diagram

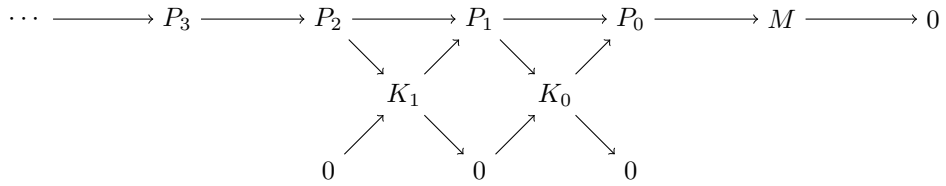
$$\begin{array}{ccccc} 0 & \longrightarrow & \mathrm{Hom}_S(B, \mathrm{Hom}_R(S, I)) & \longrightarrow & \mathrm{Hom}_S(A, \mathrm{Hom}_R(S, I)) \\ & & \downarrow \cong & & \downarrow \cong \\ 0 & \longrightarrow & \mathrm{Hom}_R(B \otimes_S S, I) & \longrightarrow & \mathrm{Hom}_R(A \otimes_S S, I) \\ & & \downarrow \cong & & \downarrow \cong \\ 0 & \longrightarrow & \mathrm{Hom}_R(B, I) & \longrightarrow & \mathrm{Hom}_R(A, I) \end{array}$$

[13] I'm almost entirely positive that these details are easy, and I don't want to do them.

with all vertical maps being isomorphisms. Since I is an injective module, the bottom row is exact, and so by commutativity and Proposition 299, all three rows are exact, and in particular, the map $\mathrm{Hom}_S(B, \mathrm{Hom}_R(S, I)) \to \mathrm{Hom}_S(A, \mathrm{Hom}_R(S, I))$ is injective, which proves that the functor $\mathrm{Hom}_S(-, \mathrm{Hom}_R(S, I))$ is exact. □

4.9.2 Projective Dimension, Regular Local Rings

Definition 316. Let M be an $R-$module. Then there exists a projective $R-$module, P_0 such that $0 \to K_0 \to P_0 \to M \to 0$ is exact, where K_0 is the kernel of the map $P_0 \to M$. That is, one first finds a surjection from a projective $R-$module to M, say $f_0 : P_0 \to M$ and then set $K_0 = \ker(f_0)$. Similarly, there exists a projective $R-$module, P_1 such that $0 \to K_1 \to P_1 \to K_0$ is exact, where K_1 is the kernel of the map $P_1 \to K_0$. Repeating in this way, gives a long exact sequence



This is called a *projective resolution* of M. The K_i's are called the *syzygyies* of M. The *projective dimension* of M is $\mathrm{pd}_R(M) = \inf\{\text{lengths of all projective resolutions of } M\} = \inf\{n \mid K_n \text{ is projective}\}$. If no projective resolution is finite, then $\mathrm{pd}_R(M) = \infty$. That is, we set $\inf \emptyset = \infty$.

Theorem 317 (Hilbert's Syzygy Theorem (1890))**.** *If $R = k[x_1, \ldots, x_n]$ where k is a field, then $\mathrm{pd}_R(M) \leq n$ for every $R-$module M.*

Remark 318. Note in the previous theorem, that $n = \dim R$ and $\mathfrak{m} = (x_1, \ldots, x_n)$ is a maximal ideal.

Theorem 319 (Krull)**.** *Let $(R, \mathfrak{m})$ be a local ring. Then $\mu_R(\mathfrak{m}) \geq \dim R$.*

Definition 320. If $\mu_R(\mathfrak{m}) = \dim R$, then R is called a *regular local ring* (RLR).

Example 321. Some examples of regular local rings:

- ▷ The ring $k[x_1, \ldots, x_n]_{(x_1, \ldots, x_n)}$ where k is a field is a regular local ring.
- ▷ Any field is a regular local ring.
- ▷ Local PID's are regular local rings.
- ▷ In particular $\mathbb{Z}_{(p)}$ is a regular local ring for any prime p.

Remark 322. Here are some properties of regular local rings:

- ▷ Every regular local ring is a domain.
- ▷ Every regular local ring is a UFD.
- ▷ If $\mathfrak{m} = (x_1, \ldots, x_d)$ is the unique maximal ideal with $d = \dim R$, then $(x_{i_1}, \ldots, x_{i_k})$ is a prime ideal for all $k \leq d$ with $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, d\}$.

Question. If $(R, \mathfrak{m})$ is a regular local ring and $P \in \mathrm{Spec}\, R$, is R_P a regular local ring?[14]

Theorem 323 (Serre-Auslander-Buchsbaum, 1957)**.** *Let $(R, \mathfrak{m})$ be a local ring. The following are equivalent.*

1. *R is a regular local ring,*
2. *$\mathrm{pd}_R(M) < \infty$ for all $R-$modules, M,*
3. *$\mathrm{pd}_R(M) \leq \dim R$ for all $R-$modules, M, and*
4. *$\mathrm{pd}_R(R/\mathfrak{m}) < \infty$*

Answer. We're now able to answer the question using the Serre-Auslander-Buchsbaum Theorem (Theorem 323). To that end, let $q \in \mathrm{Spec}(R)$ and choose a projective resolution

$$0 \to P_n \to \ldots \to P_1 \to P_0 \to R/q \to 0.$$

There is a finite resolution due to Theroem 323 since R/q is an $R-$module and R is a regular local ring. Localizing at q gives a sequence of projective R_q-modules by Corollary 229. Thus, $\mathrm{pd}_{R_q} R_q/qR_q \leq n < \infty$ and so R_q is a regular local ring by Theorem 323.

[14] This was an open question for a long time.