Introduction to Rings and Modules

Lecture 23, Friday June 30 2023

Ari Feiglin

Lemma 23.0.1 (Brauer's Lemma):

If R is a ring (not necessarily commutative) and $(0) \neq I \trianglelefteq R$ is a minimal left ideal, suppose $I^2 \neq (0)$ then there exists an idempotent element $e \in R$ such that

(1) $I = Re$

(2) eRe is a division ring

Proof:

Since $I^2 = \{\sum_{k=0}^n y_k x_k \mid x_k, y_k \in I\}$, there exist $x, y \in I$ such that $yx \neq 0$. Let us focus on $Ix = \{ax \mid a \in I\}$, we claim that this is a left ideal of R. Since if $ax, bx \in Ix$ then $ax + bx = (a+b)x \in Ix$ and if $ax \in Ix$ and $b \in R$ then $b(ax) = (ba)x \in Ix$ since I is a left ideal. Thus Ix is closed under addition and multiplication by R as required. And since $y \in I$ and $yx \neq 0$ we have $Ix \neq (0)$.
Thus we have that $(0) \neq Ix \subseteq Rx \subseteq I$. And since I is minimal we have $Ix = Rx = I$. And since $x \in I$ this means $x \in Ix$ and so there exists an $e \in I$ such that $x = ex$. We will show that e has the desired properties.
Notice that

$$e^2x = e(ex) = ex = x$$

and so

$$(e^2 - e)x = x - x = 0$$

and thus $e^2 - e \in \mathrm{Ann}_R(x) = \{r \in R \mid rx = 0\}$ which is a left ideal of R. And so $I \cap \mathrm{Ann}_R(x)$ is a left ideal of R, but since $e \in I$ and $ex = x \neq 0$, $e \notin \mathrm{Ann}_R(x)$ and so $I \cap \mathrm{Ann}_R(x)$ is a proper subset of I, and since I is minimal this means that $I \cap \mathrm{Ann}_R(x) = (0)$, but $e^2 - e \in I \cap \mathrm{Ann}_R(x)$ and so $e^2 = e$, meaning e is idempotent as required.
Now we claim $I = Re$. Obviously $Re \subseteq I$ since $e \in I$, and since $e \neq 0$ (since $ex = x \neq 0$) we have $Re \neq (0)$ is a non-zero ideal. By I's minimality this means $I = Re$.
Now we claim that eRe is a division ring. We showed last lecture that $e \in eRe$ is its identity, so let $0 \neq eae \in eRe$ for some $a \in R$. Then $eae \in eRe \subseteq Re = I$, and thus $(0) \neq Reae \subseteq I$, meaning $I = Reae$, and since $e \in I$ this means there exists a $r \in R$ such that $reae = e$. And so $ere \in eRe$, and

$$(ere)(eae) = ereae = e(reae) = e^2 = e$$

And so every element in eRe has a left inverse, and we know this means that every element in eRe has an inverse (if every element of R has a left inverse, then every element of R has an inverse: let $a \in R$ then there exists a $b \in R$ such that $ba = 1$, but there also exists a $c \in R$ such that $cb = 1$. And so $c(ba) = c$ and $(cb)a = a$ so $a = c$ and in particular $ba = ab = 1$.) Thus eRe is a division ring. ∎

We claim that if D is a division ring and M is a (left/right) D-module, then M is free (has a basis) and all two bases of M have the same cardinality. We proved this in linear algebra for fields (commutative division rings), the proof here is the same.

Theorem 23.0.2 (Wedderburn's Theorem):

Suppose R is a simple ring, then if R has a minimal left ideal then there exists an $n \in \mathbb{N}$ and a division ring D such that $R \cong M_n(D)$.

Proof:

Let I be R's minimal left ideal. Then $I = RI$, and on the other hand IR is a two-sided ideal of R. This is because if

$b \in IR$ then $b = \sum_{k=0}^{n} i_k r_k$, and if $r \in R$:

$$rb = \sum_{k=0}^{\infty} (ri_k) r_k \in IR$$

since I is a left ideal so $ri_k \in I$. And

$$br = \sum_{k=0}^{\infty} i_k (r_k r) \in IR$$

But since $I \neq (0)$, $IR \neq (0)$. But R is simple so $IR = R$.
Thus

$$R = RR = IRIR = I(RI)R = I^2 R$$

And so $I^2 \neq (0)$, so by **Brauer's Lemma** there exists an idempotent $e \in R$ such that $I = Re$ and eRe is a division ring. Let us denote $D = eRe$. Since $D \subseteq Re = I$, and I is closed under multiplication by its own elements (from the left and right), it is closed under multiplication by elements of D. Thus I can be given the structure of a right D-module by $a \cdot d = ad$.
Let $\mathrm{End}_D(I)$ be the set of all endomorphisms of I as a D-module, then we claim $R \cong \mathrm{End}_D(I)$. Let us define a function

$$\varphi \colon R \longrightarrow \mathrm{End}_D(I), \quad \varphi(r) = \varphi_r$$

where

$$\varphi_r \colon I \longrightarrow I, \quad \varphi_r(a) = ra$$

φ_r is well-defined since $ra \in I$ so φ_r is indeed a function over I, and φ is well-defined since

$$\varphi_r(a+b) = r(a+b) = ra + rb = \varphi_r(a) + \varphi_r(b)$$

and

$$\varphi_r(ad) = r(ad) = (ra)d = \varphi_r(a)d$$

Thus $\varphi(r) \in \mathrm{End}_D(I)$ as required. We further claim that φ is actually an isomorphism. It is a homomorphism since

$$\begin{aligned} \varphi_{r+s}(a) = (r+s)a = ra + sa = \varphi_r(a) + \varphi_s(a) &\implies \varphi(r+s) = \varphi(r) + \varphi(s) \\ \varphi_{rs}(a) = rsa = r(sa) = \varphi_r(\varphi_s(a)) &\implies \varphi(rs) = \varphi(r) \circ \varphi(s) \\ \varphi_1(a) = 1a = a &\implies \varphi(1) = \mathrm{id} \end{aligned}$$

φ is injective since if $r \in \mathrm{Ker}(\varphi)$ then $\varphi_r = 0$. Recall $IR = R$, and so $rI = (0)$, and $rR = rIR = (0)$, but if $r \neq 0$ then $r \in rR$ and so $rR \neq (0)$ meaning $r = 0$, so $\mathrm{Ker}(\varphi) = (0)$ as required.
Now suppose $\psi \colon I \longrightarrow I$ is a function such that $\psi \in \mathrm{End}_D(I)$. Recall $I = Re$ and so $1 \in R = IR = ReR$ and thus

$$1 = \sum_{i=1}^{m} r_i e s_i$$

for $r_i, s_i \in R$. Let $a \in I$ then since $I = Re$, we have $a = be$ for $b \in R$ and thus

$$\psi(a) = \psi(be) = \psi(1 \cdot be) = \psi\left(\sum_{i=1}^{m} r_i e s_i b e\right)$$

the summands are in $Re = I$ and so

$$= \sum_{i=1}^{m} \psi(r_i e s_i b e) = \sum_{i=1}^{m} \psi(r_i) e s_i b e = \left(\sum_{i=1}^{m} \psi(r_i) e s_i\right) be$$

Let the sum be equal to r, and so we have that

$$\psi(a) = r \cdot be = ra$$

and so $\psi = \varphi(r)$, meaning φ is surjective. Thus φ is an isomorphism, $R \cong \mathrm{End}_D(I)$.
Now, since I is a D-module, it is free. We claim it is also finitely-generated. Let

$$J = \{\varphi \in \mathrm{End}_D(I) \mid \varphi(I) \text{ is a finitely-generated } D\text{-module}\}$$

We claim that J is a two-sided ideal of $\mathrm{End}_D(I)$. Let $\varphi_1, \varphi_2 \in J$ then $\varphi_1(I)$ and $\varphi_2(I)$ are both finitely generated and so if we take the union of generating sets of theirs, we get a finite set which generates $\varphi_1(I) + \varphi_2(I) = (\varphi_1 + \varphi_2)(I)$. And if $\psi \in \mathrm{End}_D(I)$ and $\varphi \in J$ then suppose $I = a_1 D + \cdots + a_n D$, so

$$(\psi \circ \varphi)(I) = \psi(\varphi(I)) = \psi(a_1 D + \cdots + a_n D) = \psi(a_1)D + \cdots + \psi(a_n)D$$

and so $\psi \circ \varphi(I)$ is also finitely-generated. And

$$(\varphi \circ \psi)(I) = \varphi(\psi(I)) \subseteq \varphi(I)$$

and so $\varphi \circ \psi, \psi \circ \varphi \in J$. Thus $J \trianglelefteq \mathrm{End}_D(I)$ is a two-sided ideal as required.
Let B be a basis of I, and let $b \in B$ then

$$I \cong bD \times \langle B \setminus \{b\} \rangle$$

then we can define $\psi \colon I \longrightarrow bD$ which projects elements of I to their component in bD. ψ is an endomorphism, and $\psi(I) = bD$ which is a cyclic D-module, and therefore finitely-generated so $\psi \in J$, and in particular $J \neq (0)$. But since $\mathrm{End}_D(I) \cong R$ which is simple, $J = \mathrm{End}_D(I)$. And since $\mathrm{id} \in \mathrm{End}_D(I)$, this means that $\mathrm{id}(I) = I$ is finitely-generated as a D module.
Let $b_1, \ldots, b_n$ be a basis of I as a D-module, then we can construct an isomorphism

$$R \cong \mathrm{End}_D(I) \cong M_n(D)$$

since endomorphisms over a finitely generated module are isomorphic to matrices (as shown in linear algebra).

■