Abstract Algebra Lecture Notes

Simon Xiang

Lecture notes for the Fall 2020 graduate section of Abstract Algebra (Math 380C) at UT Austin, taught by Dr. Ciperiani. I'm currently auditing this course due to the fact that I'm not officially enrolled in it. These notes were taken live in class (and so they may contain many errors). You can view the source code here: https://git.simonxiang.xyz/math_notes/file/freshman_year/abstract_algebra/master_notes.tex.html.

Contents

Lecture 1

November 23, 2020

Came a little late, was making a big matrix.

1.1 Sums, products, and finitely generated modules

Note. A note on notation. We denote the set of R-module homomorphisms from $M \to N$ by $\mathrm{Hom}_R(M,N)$. You can verify in your free time that $\mathrm{Hom}_R(M,N)$ is itself an R-module.

Proposition 1.1. *Let M,N be R-modules and $\varphi\colon M \to N$ be an R-module homomorphism. Then*

1. *missed it*

Definition 1.1. Let M be an R-module and N be an R-submodule of M. Then

$$M/N = \{m+N \mid m \in M\}$$

is an R-module. We say that M/N is the **quotient module** of M by N.

To verify that M/N is an R-module, we need to show that:

1. M is an abelian group, N a subgroup implies that M/N is an abelian group.
2. The map $R \times M/N \to M/N$ defined by $(r, m+N) \mapsto rm+N$ satisfies the necessary properties.

Theorem 1.1. *Let R be a ring, M,N be R-modules, and $\varphi\colon M \to N$ be an R-module homomorphism. Then $M/\ker\varphi \simeq \operatorname{im}\varphi$.*

Definition 1.2. Let R be a ring, M an R-module, and A,B be submodules of M. Then

$$A+B := \{a+b \mid a \in A, b \in B\}$$

is a submodule of M.

Definition 1.3. Let R be a ring, M be an R-module, and $A \subseteq M$. Then

$$RA := \begin{cases} 0 & \text{if } A = \emptyset, \\ \{\sum_{i=1}^n r_i a_i \mid r_i \in R, a_i \in A\} & \text{otherwise} \end{cases}$$

is an R-submodule of M. We say that RA is **generated** by A, or that A is a **generating set** for RA. We won't give any examples, because you already have plenty from linear algebra (consider the spanning set, etc). We also say that a submodule N of M is **finitely generated** if there exists a finite set A such that $N = RA$.

Example 1.1 (Direct sums and products)**.** As a $\mathbb{Q}$-module, $\mathbb{R}^n$ is *not* finitely generated, but $\mathbb{Q}^n \subseteq \mathbb{R}^n$ a submodule of $\mathbb{R}^n$ *is* finitely generated.

Definition 1.4. Let R be a ring, and $M, \cdots, M_k$ be R-modules. Then $M_1 \times \cdots \times M_k$ is an R-module with respect to componentwise addition and multiplication by $r \in R$. More generally, let $\{M_i \mid i \in I\}$ be R-modules. Then

$$\bigoplus_{i\in I} M_i := \left\{ \sum_{i\in I} a_i \,\middle|\, a_i = 0 \text{ for all but finitely many } i \in I \right\}$$

is an R-module, and we call this the **direct sum** of the M_i. Similarly,

$$\prod_{i\in I} := \left\{ (a_i)_{i\in I} \,\middle|\, a_i \in M_i \right\}$$

is defined as the **direct product** of the M_i for $i \in I$ and is also an R-module.

Proposition 1.2. *Let M be an R-module, $N_1, \cdots, N_K$ be submodules of M. Then the map*

$$\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k, \quad (n_1, \cdots, n_k) \mapsto n_1 + \cdots n_k$$

is a surjective R-module homomorphism.

Note. Note that π is injective iff $x \in N_1, \cdots, N_k$ is written uniquely as a sum $x = \sum_{i=1}^{n} n_i$ with $n_i \in N_i$ iff $N_i \cap (N_1 + \cdots + \hat{N}_i + \cdots N_k) = 0$ for all i.

Definition 1.5 (Free generators)**.** An R-module is **free** on the subset $A \subseteq M$ if for all $x \in M$, there exists a unique $(a_1, \cdots, a_n) \in A$ and unique $r_1, \cdots, r_n \in R$ such that $x = r_1 a_1 + \cdots + r_n a_n$. Then we say that A is a set of **free generators** of M.

1.2 Simple modules and Schur's Lemma

Definition 1.6 (Simple modules)**.** A R-module M is **simple** if its only submodules are 0 and itself.

In group theory, simple groups are somewhat complicated, but for modules it's much "simpler" (hahaha) because we're dealing with *abelian* groups.

Proposition 1.3. *A simple R-module is isomorphic to R/m for some m a maximal ideal of R or R itself.*

Proof. Let M be a simple R-module. If $M = 0$, then $M = R/R$ so check. If $M \neq 0$, then we have some $x \in M \setminus \{0\} \implies Rx \subseteq M$, but $Rx \neq 0$ since $x \neq 0$, so $Rx = M$ since M is simple. In essence, every non-zero element generates M. Consider the map $\varphi : R \to Rx$, $r \mapsto rx$. Set $m = \ker\varphi$, this is an ideal of R. If this ideal isn't maximal, then $Rx \simeq R/\ker\varphi$ as R-modules (OK not sure if my logic is right here). ⊠

Note. The second item is presented without much context, and it's up to you to sit down and wrap your head around it (also very important).

1. An R-submodule of R is an ideal of R.
2. Submodules of $R/\ker\varphi$ are in bijection with the ideals $I \subseteq R$ such that $I \supseteq \ker\varphi$.

Hence M is simple iff $\ker\varphi$ is maximal.

Lemma 1.1 (Schur's Lemma)**.** *Let R be a ring, M, N be simple R-modules. Then any non-zero homomorphism $\varphi : M \to N$ is an isomorphism.*

Proof. Now $\ker\varphi = 0$ whenever $\ker\varphi$ is a submodule of M and $\varphi \neq$ the zero map. Furthermore, $\operatorname{im}\varphi$ is a submodule of N and $\varphi \neq 0$ means that $\operatorname{im}\varphi = N$ since N is simple. So $\ker\varphi = 0$ and $\operatorname{im}\varphi = N$ together imply that φ is 1-1 and onto, and therefore an isomorphism. ⊠

Lecture 2

November 30, 2020

What's a tensor? It's how to create a third module from two other modules.

2.1 Noetherian modules

Definition 2.1 (Noetherian modules)**.** Let M be a (left) R-module for R a ring. Then M is **Noetherian** R-module if it satisfies the ascending chain condition on submodules, ie every sequence of submodules

$$M_1 \subseteq M_2 \subseteq \cdots$$

has a maximal element M_m, ie $M_k = M_m$ for all $k \geq m$. This is the same idea we talked about with Noetherian rings, in which every ascending chain of ideals terminates.

Note. A ring R is Noetherian iff R is Noetherian as an R-module, since R-submodules of R are just ideals of R.

Theorem 2.1. *Let R be a ring, and M be an R-module. Then TFAE:*

1) *M is Noetherian,*

2) *Every non-empty set of submodules of M contains a maximal element with respect to inclusion,*

3) *Every submodule of M is finitely generated, in particular, M itself is finitely generated.*

Proof. The proof is the same as the one for Noetherian rings, it's also in the book. ⊠

Definition 2.2 (Rank)**.** Let R be an integral domain, M be an R-module. We define the notion of $\operatorname{rank} M :=$ maximal number of linear independent elements of M. Recall that $\{m_1, \cdots, m_k\} \subseteq M$ are linearly independent if $r_1 m_1 + \cdots + r_k m_k = 0 \implies r_1 = \cdots = r_k = 0$.

Proposition 2.1. *Let R be an integral domain, and M be a free R-module of rank $n < \infty$. Then any $n+1$ elements of M are linearly dependent over R.*

Proof. Let $F := \operatorname{Frac}(R)$, and M be free of rank n, which means that $M \simeq \overbrace{R \times \cdots \times R}^{n \text{ copies}} \hookrightarrow F \times \cdots \times F$, $M \hookrightarrow F^n$, an n-dimensional vector space over F. Then $(n+1)$ elements of M $\{m_1, \cdots, m_{n+1}\} \subseteq M \hookrightarrow F^n$ implies that $\{m_1, \cdots, m_{n+1}\}$ are linearly independent over F. Then there exist $(\alpha_1, \cdots, \alpha_{n+1}) \in F^{n+1} \backslash \{0\}$ such that $\sum_{i=1}^{m+1} \alpha_i m_i = 0$, and $\alpha_i \in F$ implies that $\alpha_i = a_i / b_i$ for $a_i, b_i \in R$, $b_i \neq 0$ for all i. Then

$$\sum_{i=1}^{n+1} r_i m_i = 0 \text{ with } r_i = a_i \frac{b}{b_i} \text{ where } b = \prod_{i=1}^{n+1} b_i.$$

So $(r_1, \cdots, r_{n+1}) \in R^{n+1} \setminus \{0\}$ since R is an integral domain, which is what we wanted. ⊠

2.2 Annihilators and torsion

Definition 2.3 (Torsion)**.** Let R be an integral domain, M be an R-module. Then we define the **torsion submodule** as

$$\operatorname{Tor} M := \{m \in M \mid rm = 0 \text{ for some } r \in R \setminus 0\}$$

Note that this is defined as a set, but you can indeed verify that this is a submodule of R. If M is free, then $\operatorname{Tor} M = 0$, since there are no relations on any m.

Definition 2.4 (Annihilator)**.** Let N be a submodule of M an R-module. Then we define the **annihilator** of N as

$$\operatorname{Ann}(N) := \{r \in R \mid rn = 0 \ \forall n \in N\}.$$

Note that $\operatorname{Ann}(N)$ is an R-ideal. If $L \subseteq N$ are both submodules of N, then we have $\operatorname{Ann}(L) \supseteq \operatorname{Ann}(N)$. Clearly the annihilator of a free module is zero, since annihilating creates relations.

Example 2.1. Note that $\operatorname{Ann}(\operatorname{Tor} M)$ may or may not be trivial. For example, let $M = \mathbb{Q}/\mathbb{Z} = \left\{\frac{a}{b} + \mathbb{Z} \mid 0 \leq a < b\right\}$ as a $\mathbb{Z}$-module (convince yourself of the equality as sets). Then $\operatorname{Tor}(M) = M$, since $b\left(\frac{a}{b} + \mathbb{Z}\right) = \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}$. So $\operatorname{Ann}(\operatorname{Tor} M) = \operatorname{Ann}(M)$, but $\operatorname{Ann}(\mathbb{Q}/\mathbb{Z}) = 0$. To see this, let $r \in \mathbb{Z}$, then $r\left(\frac{1}{r+1} + \mathbb{Z}\right) = \frac{r}{r+1} + \mathbb{Z} \neq 0$ in $\mathbb{Q}/\mathbb{Z}$. So $\mathbb{Q}/\mathbb{Z}$ is an example of a non-Noetherian $\mathbb{Z}$-module (not finitely generated).

2.3 Modules over PIDs

Now we get to state and prove the main theorem that we've been working toward.

Theorem 2.2. *Let R be a PID, M be a free module of rank m, and N a submodule of M. Then*

1) *N is free of rank $n \leq m$,*

2) *There exists a basis of M given by $\{y_1, \cdots, y_m\}$ such that $\{a_1 y_1, \cdots, a_n y_n\}$ is a basis of N with $a_1, \cdots, a_n \in R$ such that $a_1 \mid a_2 \mid \cdots \mid a_n$.*

Proof. If $N = 0$, then $M \simeq Ry_1 + \cdots + Ry_m \simeq \overbrace{R \times \cdots \times R}^{m \text{ copies}}$ since M is free of rank m and $n = 0$ (nothing left to say here, think of this as an exceptional case). Now assume that $N \neq 0$. We'll finish this next time. This result leads into a lot of useful linear algebra results. ⊠

Lecture 3

December 1, 2020

Last time, to fill in a gap M being free of rank n means by definition that M has an R-basis with n-elements.

Proof. To finish the proof of Theorem 2.2, let M be a free R-module for R a PID of rank m, and N be a nontrivial submodule of M.

Claim. N is a free module of rank $n \leq m$. Consider the R-module homomorphisms $\varphi\colon M \to R$. Then N being a submodule of M implies that $\varphi(N)$ is an R-submodule of R, so $\varphi(N) = (a_\varphi)$ with $a_\varphi \in R$. Consider the set of all such ideals

$$\sum = \left\{ \left(a_\varphi\right) \mid \varphi \in \mathrm{Hom}_R(M, R) \right\},$$

we have $\Sigma \neq \emptyset$ since $\varphi\colon m \mapsto 0$ an R-module homomorphisms for all $m \in M$ implies that $(0) \in \Sigma$, so $\Sigma \neq \emptyset$. How do we know $\Sigma \neq \{(0)\}$? M being a free module of rank m iff there exsits a set $\{x_1, \cdots, x_m\}$ an R-basis of M by definition, so consider the set of projection maps $\pi_j\colon M \to R$, $\sum_{i=1}^m r_i x_i \mapsto r_j$ which is well defined since we have an R-basis, so we have an R-module homomorphism. Then $\pi = (\pi_1, \cdots, \pi_m)\colon M \to R^m$ is the canonical R-module isomorphism. Now $N \neq 0$ says that $\pi(N) \neq 0$, which subsequently implies that $\pi_j(N) \neq 0$ for some j. The fact that $\pi_j \in \mathrm{Hom}_R(M, R)$ implies that $\Sigma \neq 0$ (not just nonempty, but also nonzero).

Since R is a PID, then R is Noetherian so Σ has a maximal element with respect to inclusion, ie there exists a homomorphism $\varphi_1\colon M \to R$ such that $\varphi_1(N)$ is not strictly contained in any other ideal of Σ. Let a_1 (formerly a_{φ_1}) $\in R$ such that $\varphi_1(N) = (a_1)$. Choose $z \in N$ such that $\varphi_1(z) = a_1$. Subclaim:

$$a_1 \mid \varphi(z) \text{ for all } \varphi \in \mathrm{Hom}_R(M, R).$$

For the proof of the subclaim, fix $\varphi \in \mathrm{Hom}_R(M \to R)$. Consider $(a_1, \varphi(z))$ an ideal of R. Since R is a PID, $(a_1, \varphi(z)) = (d)$, so $d = a_1 r_1 + \varphi(z) r_2$ with $r_1, r_2 \in R$. Consider $\varphi' = r_1\varphi_1 + r_2\varphi$, since $\varphi_1, \varphi \in \mathrm{Hom}_R(M, R)$ we have $\varphi' \in \mathrm{Hom}_R(M, R)$. $\varphi'(z) = d$ and $\varphi' \in \mathrm{Hom}_R(M, R)$ says that $\varphi'(N) \in \Sigma$ and $\varphi'(N) \subseteq (d)' \supseteq (a_1)$. By the maximality of (a_1), $a_1 = d \cdot u$ with u a unit of R. Then $(a_1, \varphi(z)) = (a_1) \implies a_1 \mid \varphi(z)$, finishing the subclaim.

Consider the projections $\pi_1(z), \cdots, \pi_m(z)$. We know $\pi_j \in \mathrm{Hom}_R(M, R)$, so by our subclaim $a_1 \mid \pi_j(z)$ for all $j \in \{1, \cdots, m\}$. So we can write $\pi_j(z) = a_1 b_j$ with $b_j \in R$, set $y_1 = \sum_{i=1}^m b_i x_i$, we get that $z = a_1 y_1$. Then $\varphi_1(z) = a_1$ implies that $\varphi_1(y_1) = 1$ since R is an integral domain. Subclaim two:

$$M \simeq Ry_1 \oplus \ker\varphi_1 \text{ by the map } \psi\colon x \mapsto (\varphi_1(x), x - \varphi_1(x) y_1).$$

For the proof of this, set $\psi_1\colon R \to Ry$, $x \mapsto \varphi_1(x) y_1$. ψ_1 is an R-module homomorphism since φ_1 is. Set $\psi_2\colon M \to \ker\varphi$, $x \mapsto x - \varphi_1(x) y_1$. Then $\psi_2(M) \subseteq \ker\varphi \iff \varphi(x - \varphi_1(x) y_1) = 0$. $\varphi_1(x - \varphi_1(x) y_1) = \varphi(x) - \varphi_1(x)\varphi_1(y_1) = \varphi_1(x) - \varphi_1(x) = 0$, so we land in the right place. $\psi_2 = \mathrm{id} - \psi_1$ both R-module homomorphisms implies that ψ_2 is an R-module homomorphism, so ψ is an R-module homomorphism as well. We need to verify that ψ is injective and surjective. $x \in M$ implies that $x = \psi_1(x) + \psi_2(x)$, so ψ is injective.

To see that ψ is surjective, note that

$$\left.\begin{aligned} \psi_1|_{Ry_1} &= \mathrm{id} \\ \psi_2|_{\ker\varphi_1} &= \mathrm{id} \end{aligned}\right\} \implies \left.\begin{aligned} &(z_1 z_2) \in Ry_1 \oplus \ker\varphi_1 \\ &\psi(z_1 + z_2) \in M = \left(\overset{=\psi_1(z_1+z_2)}{\psi_1(z_1)}, \overset{=\psi_2(z_1+z_2)}{\psi_2(z_2)} \right) \end{aligned}\right\} = (z_1, z_2) \implies \psi \text{ is surjective.}$$

Hence ψ is an R-module isomorphism. Subclaim three:

$$N \overset{\psi}{\simeq} Ra_1 y_1 \oplus N \cap \ker \varphi.$$

Proof: $\psi : N \to Ry_1 \oplus \ker \varphi$, $n \mapsto (\psi_1(n), \psi_2(n))$, $\psi_1(n) = \varphi_1(n)y_1 \in \varphi_1(N)y_1 = a_1Ry_1 = Ra_1y_1$. $\psi_2(n) \in \ker \varphi$, to show $\psi_2(n) \in N$, $\psi_2(n) = n - \psi_1(n)y_1 \in n + Ra_1y_1 \in N$.

⊠