

# Abstract Algebra Lecture Notes

Simon Xiang

Lecture notes for the Fall 2021 graduate section of Abstract Algebra (Math 380C) at UT Austin, taught by Dr. Raskin. These notes were taken live in class (and so they may contain many errors). Source files: [https://git.simonxiang.xyz/math\\_notes/files.html](https://git.simonxiang.xyz/math_notes/files.html)

## Contents

1	October 15, 2021	2
2	October 18, 2021	3
3	October 20, 2021	4
4	October 22, 2021	5
5	October 25, 2021	5
6	October 27, 2021	6
7	October 29, 2021	6

# 1 October 15, 2021

Today we finish up on roots of unity. Assume  $k$  is a field of characteristic  $p > 0$ . Last time we showed that this Frobenius map  $\varphi: k \rightarrow k, f \mapsto f^p$  is a homomorphism. If  $k = \mathbb{F}^p$ , then this Frobenius map is just the identity:  $\varphi(1) = 1, \varphi(2) = 2\varphi(1) = 2$ , and  $n^p = \varphi(n) = n$  for every  $n$ . So  $\varphi = \text{id}$ , and  $n^p = n \pmod{p}$  for every  $n \in \mathbb{Z}$ , which is **Fermat's little theorem**. But for any field  $k$  of characteristic  $p$ , there's always a map

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad} & k \\ & \searrow \quad \swarrow & \\ & \mathbb{Z}/p = \mathbb{F}_p & \end{array}$$

**Claim.**  $\mathbb{F}_p = \{f \in k \mid \varphi(f) = f\}$ .

*Proof.* The right hand side is equal to the roots of  $t^p - t$ , and there are less than or equal to  $p$  of them, and  $p$  of them in  $\mathbb{F}_p$ .  $\square$

**Lemma 1.1.** For every  $n \geq 1$ ,  $\mu_{np}(k) = \mu_n(k) \subseteq k^\times$ .

**Corollary 1.1.**  $\mu_{np^r}(k) = \mu_n(k)$  for every  $r \geq 0$ .

*Proof.* Consider the case where  $n = 1$ . Then  $\mu_p(k) = \{1\}$ . Suppose  $\zeta \in \mu_p(k)$ , so  $\zeta^p = 1$ , which implies  $\zeta^p - 1 = \varphi(\zeta) - \varphi(1) = 0$ . Therefore  $(\zeta - 1)^p = 0$  (freshman's dream in a field of characteristic  $p$ ), so  $\zeta - 1 = 0$  since we're in a domain (field). In the general case, we clearly have  $\mu_n(k) \subseteq \mu_{np}(k)$ . Conversely, if  $\zeta \in \mu_{np}(k)$ , we have  $\zeta^{np} = 1$  which implies  $(\zeta^n)^p = 1$ , which means  $\zeta^n \in \mu_p(k)$ . So by earlier,  $\zeta^n = 1$ , and  $\zeta \in \mu_n(k)$ .  $\square$

Now we can prove the rest of ?? from Monday. We showed that if  $p \nmid n$ , then there exists a field extension  $K/k$  such that  $|\mu_n(K)| = n$ . (The proof uses the fact that  $t^n - 1$  is separable). What we just showed is that if  $n = p^r m, p \nmid m$ , then there exists a  $K/k$  such that  $|\mu_n(K)| = |\mu_m(K)| = m$ .

Next we claim that for any  $n \geq 1$  and any  $k$ ,  $\mu_n(k)$  is cyclic.

*Proof.* WLOG, assume  $p \nmid n$ . Then we have some field extension  $K/k$  such that  $|\mu_n(K)| = n$ . So  $\mu_n(k) \subseteq \mu_n(K) \simeq \mathbb{Z}/n$  by last time. Any subgroup of  $\mathbb{Z}/n$  has the form of  $d\mathbb{Z}/n\mathbb{Z}$  (or  $\mathbb{Z}/(\frac{n}{d})\mathbb{Z}$ ) for some  $d \mid n$ . This proves the claim that  $\mu_n(k)$  is cyclic.

Our next claim is that any finite subgroup  $G \subseteq k^\times$  is cyclic. For every  $g \in G$ ,  $g^{|G|} = 1$ . This implies  $G \subseteq \mu_{|G|}(k)$ . By the same argument,  $G$  is cyclic.  $\square$

Again, the main corollary is that  $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)$ . The same applies as is for any finite field  $k$ , i.e.,  $k^\times \simeq \mathbb{Z}/(|k|-1)\mathbb{Z}$ .

This ends our whole schpeal on finite fields. Now we'll explain some constructions with finite groups, probably using this result, and then move on to modules over PIDs. There is a slogan, which is that finite groups get more complicated the more prime factors they have.

0	* the trivial group
1	$\mathbb{Z}/p$ for some $p$
2	$\mathbb{Z}/p \times \mathbb{Z}/p, \mathbb{Z}/p^2, \mathbb{Z}/p \rtimes \mathbb{Z}/q$ the semidirect product

Figure 1: Groups get more complicated the more prime factors they have.

What is a semidirect product? Good question. Given two groups  $G, H$  and an action of  $G$  on  $H$  by a group automorphism, for every  $g \in G$  the map  $H \xrightarrow{\sim} H$  (act by  $g$ ) is a group homomorphism/automorphism. This is the

main example to keep in mind: if  $k$  is a commutative ring, take  $G = (k^\times, \text{mult})$  and  $H = (k, +)$ . So  $G$  acts on  $H$  via multiplication. Note that for  $\lambda \in k^\times$ ,  $k \xrightarrow{\lambda \cdot (-)} k$  is a group homomorphism (distributive property of multiplication).

**Note.** A note on notation. For  $g \in G$ , the automorphism  $H \xrightarrow{\text{act by } g} H$  is denoted by  $h \mapsto {}^g h$ .

Some basic identities.  ${}^g(h_1 h_2) = ({}^g h_1)({}^g h_2)$ , also  ${}^{g_1 g_2}(h) = {}^{g_1}({}^{g_2} h)$ . Furthermore  ${}^g(1) = 1$ , and  ${}^1 h = h$ .

## 2 October 18, 2021

This is the setup- let  $G, H$  be groups, and let  $G$  act on  $H$  by group automorphisms. For  $g \in G, h \in H$ ,  $h \mapsto {}^g h$  is the action of  $g$ . This leads to a new group  $G \ltimes H$  that does something- what is this something? An action of  $G \ltimes H$  is the data of an action of  $G$  and an action of  $H$  such that something natural happens.

**Example 2.1.** Let  $G = \mathbb{Z}/2, H = \mathbb{Z}, X = \mathbb{Z}$ . Then  $G$  acts on  $H$  by group automorphisms (denote this action  $\sigma$ ), where  $\sigma: n \mapsto -n$ . We also have a  $\mathbb{Z}$ -action  $\tau$  (shift up by 1), then  $(\sigma\tau)(n) = \sigma(n+1) = -n-1 = \tau^{-1}(-n) = \tau^{-1}\sigma(n) = \sigma\tau(\sigma(n))$ .

The setup in general goes like this: an action of a semidirect product  $G \ltimes H$  on  $X$  is an action of  $G, H$  such that for every  $g \in G, h \in H, x \in X$ ,  $g(h(x)) = {}^g h \cdot (gx)$ . Heuristic: we want the formula  $ghg^{-1} = {}^g h$  to make sense and be true in  $G \ltimes H$ . So how do we construct  $G \ltimes H$ ?

**Definition 2.1.** Consider the setup in the beginning, where  $G, H$  are groups and  $G$  acts on  $H$  by automorphisms. Let the **semidirect product**  $G \ltimes H = G \times H$  as a set, with group multiplication

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 \cdot {}^{g_1} h_2).$$

**Example 2.2.** If  $G$  acts on  $H$  trivially, then  $G \ltimes H = G \times H$ .

The claim is that this indeed forms a group. To check associativity, we have

$$\begin{aligned} (g_1, h_1) \cdot [(g_2, h_2) \cdot (g_3, h_3)] &= (g_1, h_1) \cdot (g_2 g_3, h_2 {}^{g_2} h_3) \\ &= (g_1 g_2 g_3, h_1 {}^{g_1} (h_2 {}^{g_2} h_3)) \\ &= (g_1 g_2 g_3, h_1 {}^{g_1} h_2 {}^{g_1 g_2} h_3) = \dots \end{aligned}$$

**Example 2.3.** Some basic structures:

- (a) We have  $H \hookrightarrow G \ltimes H, h \mapsto (1, h)$  a homomorphism. Moreover, the image is a *normal* subgroup:  $(g, 1) \cdot (1, h) \cdot (g^{-1}, 1) = (g, {}^g h) \cdot (g^{-1}, 1) = (1, {}^g h)$ . This fits into a sequence

$$0 \rightarrow H \rightarrow G \ltimes H \rightarrow G \rightarrow 0.$$

- (b)  $G \ltimes H \rightarrow G, (g, h) \mapsto g$  is a *surjective* homomorphism with kernel  $H = \{(1, h)\}$ , which implies  $H$  is normal.

- (c)  $G \rightarrow G \ltimes H, g \mapsto (g, 1)$  is a **splitting** of the map from (b), i.e.,  $G \rightarrow G \ltimes H \rightarrow G$  is the identity map.

**Note.** A note on notation:  $G \ltimes H = H \rtimes G$ , and  $K \triangleleft G$  means  $K$  is normal in  $G$ . The  $\triangleright$  in  $G \ltimes H$  tells you  $H$  is the one who is normal, which implies  $G$  is the one who acts.

Suppose we're given a space  $X$  and an action  $G \ltimes H$ . We need to check the data from before:  $H \rightarrow G \ltimes H, G \rightarrow G \ltimes H \rightsquigarrow$  actions of  $G$  and  $H$  on  $X$ . To see this,  $(g, 1) \cdot (1, h) = (g, {}^g h) = (1, {}^g h) \cdot (g, 1)$  implies that for every  $x \in X$ ,

$$\begin{aligned} g \cdot (h \cdot x) &= (g, 1)(h, 1)x \\ &= (g, {}^g h)x = (1, {}^g h)(g, 1)x \\ &= {}^g h \cdot (g \cdot x). \end{aligned}$$

Conversely, given  $G, H$  actions,  $(g, h) \cdot x = {}^g h \cdot (g \cdot x)$  defines an action if the compatibility condition holds.

**Example 2.4.** Some examples of semidirects:

- (1) Let  $G = k^\times$  act on  $k = H$ , and  $X = k$ . Then  $H$  acts on  $k$  by addition, and  $G = k^\times$  acts on  $k$  by multiplication.
- (2) For  $k = \mathbb{Z}$ , this is what we discussed at the beginning of the class.  $\mathbb{Z}^\times = \{\pm 1\} \simeq \mathbb{Z}/2$ . Then

$$G \ltimes H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in k^\times, b \in k \right\} \subseteq \mathrm{GL}_2(k).$$

- (3) Let  $G = \mathbb{Z}/2 = \{1, s\}$ ,  $H = \mathbb{Z}/n = \{1, r, r^2, \dots, r^{n-1}\}$ . Then  $G$  acts on  $H$  by  $sr = r^{-1}$ . Then  $G \ltimes H = D_{2n}$ , the dihedral group of order  $2n$ . We have  $r^i, r^i s$  and  $srs^{-1} = r^{-1}, s^2 = 1, r^n = 1$ , or  $D_{2n} = \langle r, s \mid r^n = s^2 = (sr)^2 = 1 \rangle$ .  $D_{2n}$  is setup to act on a regular  $n$ -gon by “rigid motions” (isometries in  $\mathbb{R}^3$ ).

### 3 October 20, 2021

Today we’ll talk about the recognition criterion for semidirect products.

**Definition 3.1.** Given groups  $G, H$ , an **extension** of  $G$  by  $H$  is the data  $(E, \pi, i)$  where  $E$  is a group,  $\pi: E \twoheadrightarrow G$ ,  $i: H \hookrightarrow E$ , and we have that  $\pi i(y) = 1$  for every  $h \in H$ . Then the map  $H \xrightarrow{i} \ker(\pi) \subseteq E$  is an isomorphism, and  $\pi$  is surjective iff  $E/\ker(\pi) \xrightarrow{\sim} G$  iff  $E/H \xrightarrow{\sim} G$ . In short,  $E$  is a group,  $H \subseteq E$  is normal, and  $E/H \simeq G$ .

**Note.** A note on notation. We write  $1 \rightarrow H \xrightarrow{i} E \xrightarrow{\pi} G \rightarrow 1$ , with an exception by replacing the 1s with 0s. The group  $H$  (resp  $G$ ) is uniquely written positively (resp  $G$ ). A sequence like this is a **short exact sequence** (or SES for short) of groups.

**Example 3.1.** Some examples of short exact sequences:

- (1)  $0 \rightarrow \mathbb{Z}/2 \xrightarrow{1 \mapsto 2} \mathbb{Z}/4 \xrightarrow{1 \mapsto 1} \mathbb{Z}/2 \rightarrow 0$  is a short exact sequence.
- (2)  $0 \rightarrow \mathbb{Z}/2 \xrightarrow{x \mapsto (x, 0)} \mathbb{Z}/2 \times \mathbb{Z}/2 \xrightarrow{(x, y) \mapsto y} \mathbb{Z}/2 \rightarrow 0$  is a short exact sequence.
- (3) For every  $n, m \geq 1$ ,  $0 \rightarrow \mathbb{Z}/n \xrightarrow{1 \mapsto m} \mathbb{Z}/nm \xrightarrow{1 \mapsto 1} \mathbb{Z}/m \rightarrow 0$  is a short exact sequence.
- (4) For every  $G, H$ , we have  $1 \rightarrow H \xrightarrow{h \mapsto (1, h)} G \times H \xrightarrow{(g, h) \mapsto g} G \rightarrow 1$  is a short exact sequence.
- (5) Suppose  $G$  acts on  $H$  by group automorphisms. Then by last time,  $1 \rightarrow H \xrightarrow{h \mapsto (1, h)} G \ltimes H \xrightarrow{(g, h) \mapsto g} G \rightarrow 1$  is a short exact sequence.

**Principle.**  $G \ltimes H$  is the simplest extension of  $G$  by  $H$ .

**Definition 3.2.** A **map of extensions** of  $G$  by  $H$  is a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & H & \xrightarrow{i_1} & E_1 & \xrightarrow{\pi_1} & G \longrightarrow 1 \\ & & \downarrow \mathrm{id} & & \downarrow f & & \downarrow \mathrm{id} \\ 1 & \longrightarrow & H & \xrightarrow{i_2} & E_2 & \xrightarrow{\pi_2} & G \longrightarrow 1 \end{array}$$

for  $f$  a homomorphism.

**Lemma 3.1.** Any map  $f: E_1 \rightarrow E_2$  is a group isomorphism, and  $f^{-1}$  is a map of extensions. *todo:finish*

## 4 October 22, 2021

## 5 October 25, 2021

Digression for today and maybe tomorrow: we'll talk about Fermat's two square theorem, which is an application of previous ideas we've discussed (this is a cookie??).

**Theorem 5.1** (Fermat). *Let  $p$  be an odd prime, then there exist integers  $\alpha, \beta \in \mathbb{Z}$  such that  $p = \alpha^2 + \beta^2$  iff  $p \equiv 1 \pmod{4}$ .*

*Proof (partial).* We have  $p$  odd, so  $p \equiv$  either 1 or 3  $\pmod{4}$ . For every  $\alpha \in \mathbb{Z}$ ,  $\alpha^2 \equiv 0, 1 \pmod{4}$ . If  $\alpha$  is even, then  $4 \mid \alpha^2 \implies \alpha^2 \equiv 0 \pmod{4}$ , and  $\alpha$  odd implies  $\alpha = 2k + 1 \implies \alpha^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4}$ . Any number that is 3  $\pmod{4}$  is not the sum of two squares. This is the easy direction.  $\square$

The other direction is way more subtle. Experimentally, consider the following table:

$p$	$\alpha^2 + \beta^2$
3	bad
5	$2^2 + 1^2$
7	bad
11	bad
13	$3^2 + 2^2$
17	$4^2 + 1^2$
19	bad
23	bad
29	$5^2 + 2^2$
$\vdots$	$\vdots$
61	$6^2 + 5^2$
$\vdots$	$\vdots$

Figure 2: Checking Fermat's two square theorem.

For example,  $21 \equiv 1 \pmod{4}$  but is not the sum of two squares, so primeness is a crucial hypothesis. The key ingredient to proving this consists of things we have already done.

**Definition 5.1.** Define the ring of **Gaussian integers**  $\mathbb{Z}[i] \subseteq \mathbb{C}$  by  $\{a + bi \mid a, b \in \mathbb{Z}\}$ .

**Lemma 5.1.** *We have  $\mathbb{Z}[i] \simeq \mathbb{Z}[t]/t^2 + 1$ .*

*Proof.* There exists a unique homomorphism  $\mathbb{Z}[t] \xrightarrow{t \mapsto i} \mathbb{Z}[i]$  which factors through  $\mathbb{Z}[t]/t^2 + 1$ . The resulting map is obviously surjective, and injectivity follows from a previous homework, where we showed that every element of  $\mathbb{Z}[t]$  mod a monic degree two polynomial can be *uniquely* written as  $a + b \cdot t$ , with  $a, b \in \mathbb{Z}$ .  $\square$

**Theorem 5.2.** *The Gaussian integers  $\mathbb{Z}[i]$  are a Euclidian domain.*

Recall that this implies the Gaussian integers are a PID. We will prove Theorem 5.2 later, but for now let us assume it's true. We can deduce Fermat's theorem from here.

*Proof of Theorem 5.1.* Let  $p$  be an odd prime where  $p \equiv 1 \pmod{4}$ . We want to show there exists  $\alpha, \beta \in \mathbb{Z}$  such that  $p = \alpha^2 + \beta^2$ .

**Lemma 5.2.**  $\mathbb{Z}[i]_p$  is not a prime ideal if  $p \equiv 1 \pmod{4}$ .

*Proof of Lemma 5.2.* It suffices to show that  $\mathbb{Z}[i]/p\mathbb{Z}[i]$  is not a domain. We have  $\mathbb{Z}[i]/p\mathbb{Z}[i] = \mathbb{Z}[t]/(p, t^2 + 1) = \mathbb{Z}/p[t]/(t^2 + 1) = \mathbb{F}_p[t]/(t^2 + 1)$ . By last week's homework, when  $p \equiv 1 \pmod{4}$  in  $\mathbb{F}_p$  there exists a  $\sqrt{-1} \in \mathbb{F}_p$ . This implies  $t^2 + 1$  factors into  $(t + \sqrt{-1})(t - \sqrt{-1}) \in \mathbb{F}_p[t]$ , which implies  $\mathbb{F}_p[t]/(t^2 + 1) \simeq \mathbb{F}_p[t]/(t + \sqrt{-1}) \times \mathbb{F}_p[t]/(t - \sqrt{-1})$  (by the remainder theorem, an old hw) which is just  $\mathbb{F}_p \times \mathbb{F}_p$ . This quotient is not an integral domain, since  $(1, 0) \cdot (0, 1) = (0, 0)$ , so  $(p)$  is not prime in  $\mathbb{Z}[i]$ .  $\square$

The big idea is that modding out by a reducible polynomial leads to something that is not a field. Assuming Theorem 5.2, because  $\mathbb{Z}[i]$  is a Euclidian domain (and PID), we have  $p = x \cdot y$  for some  $x, y \in \mathbb{Z}[i]$  non-units by Lemma 5.2. Note that we can't have  $x, y \in \mathbb{Z}$ . Assume that the complex conjugate  $\bar{x} \neq x$ , also  $|\bar{x}| \neq 1$  since if this were true, this implies that for  $x = a + bi$ ,  $a^2 + b^2 = 1$ , which implies  $a = \pm 1, b = 0$  or  $a = 0, b = \pm 1$ , which implies  $x \in \{1, i, -1, -i\} \subseteq \mathbb{Z}[i]^\times$ . So  $|x|^2 = x \cdot \bar{x} \in \mathbb{Z}$ , and  $p^2 = |p|^2 = |x|^2 \cdot |y|^2$ . We have  $|x|^2, |y|^2 \in \mathbb{Z} > 1$ , which implies  $|x|^2 = |y|^2 = p$ . So if  $x = \alpha + \beta i$ , then  $|x|^2 = \alpha^2 + \beta^2 = p$ , and we are done.  $\square$

**Remark 5.1.** If  $|x|^2 = p$ , this implies  $x$  is irreducible, since  $x = x_1 x_2, |x_i|^2 = 1$  for some  $i = 1, 2$ , which subsequently implies that  $x_i \in \mathbb{Z}[i]^\times$ .

Now to prove Theorem 5.2. We'll do this next time.

## 6 October 27, 2021

## 7 October 29, 2021

Today we'll talk about modules, the goal being the classification of modules over a PID. The motivation is the following: no one gets excited over the definition of a module. Modules are organizational tools, and serve many purposes:

- (1) Many interesting problems can be phrased in terms of modules. Module theory leads to tools (induction, extensions, homological algebra, ...).
- (2) Properties of modules in the aggregate tell you interesting things about rings.

The setup: let  $A$  be a ring, possibly non-commutative.

**Definition 7.1.** A (left) **A-module** is the data  $(M, \text{act})$  where  $M = (M, +)$  is an abelian group,  $\text{act}: A \times M \rightarrow M, a, m \mapsto a \cdot m$  such that

- $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$  for every  $a \in A, m_1, m_2 \in M$ ,
- $a \cdot (b \cdot m) = (a \cdot b) \cdot m$  for every  $a, b \in A, m \in M$ ,
- $(a + b) \cdot m = a \cdot m + b \cdot m$  for every  $a, b \in A, m \in M$ ,
- $1 \cdot m = m$  for every  $m \in M$ .

A **right A-module** is one with a map  $M \times A \rightarrow M, (m, a) \mapsto ma$  such that analogous stuff happens.

Define  $A^{\text{op}} := A$  as an abelian group, with multiplication  $a \cdot^{\text{op}} b := ba$ . This is a perfectly good procedure, so left  $A^{\text{op}}$ -modules are equivalent to right  $A$ -modules. In particular, left and right  $A$ -modules are the same when  $A$  is commutative. We think of groups acting on sets (symmetries), while we think of rings acting on modules.

**Example 7.1.** Some examples of modules:

- (1) Let  $M = A$  with  $\text{act}(a, b) := a \cdot b$ , this is an  $A$ -module.
- (2) For  $I \subseteq A$  a (left) ideal (closed under addition and multiplication on the left), then  $I$  is a submodule of  $A$ . Conversely, a submodule of  $A$  is a left ideal.
- (3) A  $\mathbb{Z}$ -module is an abelian group. Specifically, for  $M$  a  $\mathbb{Z}$ -module, then  $M$  is an abelian group, and the action must be  $(n, m) \rightarrow \underbrace{m + \cdots + m}_{n \text{ times}}$  or  $(n, m) \rightarrow \underbrace{m - \cdots - m}_{n \text{ times}}$ .
- (4) If  $A = k$  is a field, then a  $k$ -module is precisely a vector space over  $k$ .

Recall that  $G$  acting on  $X$  is the same as a map  $G \rightarrow \text{Aut}(X)$ , which is sometimes a convenient perspective. Analogously, for  $M$  an abelian group, define  $\text{End}_{\text{gps}}(M) := \{\varphi : M \rightarrow M \mid \varphi \text{ is a homomorphism}\}$ . Then  $\text{End}(M)$  is naturally a ring, where for  $\varphi_1, \varphi_2 \in \text{End}(M)$ ,  $(\varphi_1 + \varphi_2)(m) := \varphi_1(m) + \varphi_2(m)$ . For  $(\varphi_1 + \varphi_2)$  to be an endomorphism, we need  $M$  to be abelian. Furthermore,  $\varphi_1 \cdot \varphi_2 := \varphi_1 \circ \varphi_2$ , i.e.,  $(\varphi_1 \cdot \varphi_2)(m) := \varphi_1(\varphi_2(m))$ . In this case,  $1 \in \text{End}(M)$  is equal to  $\text{id}_M$ . Then unwinding things, an  $A$ -module structure on  $M$  is equivalent to a ring homomorphism  $A \rightarrow \text{End}(M)$ ,  $a \mapsto \varphi_a$ , where  $\varphi_a(m) = a \cdot m$  (recall we are considering group endomorphisms, which are universal like the automorphism group).

Briefly, a **homomorphism** of  $A$ -modules is a map  $f : M \rightarrow N$  such that  $f$  is a homomorphism of abelian groups and  $f(a \cdot m) = a \cdot f(m)$  for every  $a \in A, m \in M$ . We use the same language as groups, etc a submodule is closed under stuff, an automorphism of modules is a bijective homomorphism of modules, etc.

Fix  $k$  a field, and let  $A = k[t]$ .

**Question.** What are  $k[t]$ -modules?

**Answer.** Let  $V$  be a  $k[t]$ -module. Then  $V$  is a  $k$ -module via the homomorphism  $k \rightarrow k[t]$ , also  $t \in k[t]$  determines a map  $T := (t \cdot -) : V \rightarrow V$  (the action of  $t$ ). Note that  $T$  is a linear transformation (AKA  $k$ -module endomorphism). For example,  $T(\lambda v) := (t \cdot \lambda \cdot v) = (\lambda t) \cdot v = \lambda \cdot (t \cdot v) = \lambda T(v)$  for every  $\lambda \in k, v \in V$ . Conversely, given  $V/k$  a vector space and  $T : V \rightarrow V$  a linear transformation, for  $f(t) = \sum a_i t^i \in k[t]$ ,  $f \cdot v := \sum a_i T^i(v) \in V$  defines a  $k[t]$ -module structure.

**Slogan.**  $k[t]$ -modules are vector spaces with an endomorphism.

Our goal is going to be classification of modules over PIDs. We have two great PIDs, the integers and  $k[t]$ . One corresponds to finite groups, and the other is the classification of finite dimensional vector spaces with endomorphism. This is the idea of Jordan canonical forms, giving a relationship between vector spaces with endomorphisms and ideals inside the polynomial algebra. They seem unrelated, but the connection between the two is module theory.