Math 122 - Algebra I: Theory of Groups and Vector Spaces

Taught by Hiro Tanaka
Notes by Dongryul Kim

Fall 2017

The course was taught by Hiro Lee Tanaka. The lectures were on Mondays, Wednesdays, and Fridays at 2–3pm. There was no textbook, and there were 62 students enrolled. The course had weekly problem sets, one take-home midterm, one in-class midterm, a take-home final, and an optional final paper. The course assistants were Benjamin Gunby, Dongryul Kim, Celine Liang, Roshan Padaki, and Neekon Vafa. Additional material can be found on the course website.

Contents

1 September 1, 2017

Last time we defined a group.

Definition 1.1. A **group** is the data of (G, m) where G is a set and $m : G \times G \to G$ is a function. We are going to write

$$m : (g, h) \mapsto m(g, h) = gh$$

by shorthand. This has to satisfy the conditions

(1) There exists an element $e \in G$, called the **identity** or **unit** such that $m(e, g) = g = m(g, e)$.

(2) For all $g \in G$, there exists an element $g^{-1} \in G$ such that $m(g, g^{-1}) = e = m(g^{-1}, g)$.[1]

(3) m is associative.

1.1 Properties of groups

Proposition 1.2. *Let G be a group. Suppose that there exist $g, h, k \in G$ such that $gh = gk$. Then $h = k$.*

This is a special property of a group. Take, for instance, the set of integers with multiplication. This proposition does not holds, because of 0. For any h, k, we have $0h = 0k = 0$. Indeed, the set of integers with multiplication fails (2); 0 has no inverse.

Proof. We know that there exists a $g^{-1} \in G$ such that $g^{-1}g = e$. (I'm already using shorthand.) So

$$g^{-1}(gh) = g^{-1}(gk).$$

By associativity (property (3)), we get $(g^{-1}g)h = (g^{-1}g)k$. By (2), we then get $eh = ek$. Because e is the identity, we get $h = k$. □

This was the left cancellation lemma. The right cancellation lemma also holds. If $hg = kg$, then $h = k$. The proof is almost identical and is an exercise.

A cautionary remark: in general, $m(g, h) \neq m(h, g)$, i.e., $gh \neq hg$. In the case of the integers with addition, this is true.

Example 1.3. Let G be the set of invertible 2×2 matrices:

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0 \right\}.$$

This is a group with multiplication of matrices. Then there are examples of matrices $A, B \in G$ such that $AB \neq BA$. It's a good exercise to find this example.

[1] Thank god I already defined what e is. But this is not really the case. (1) only says that there exists some e, but says nothing about uniqueness. But you can show that if there are $e, e' \in G$ satisfying (1), then $e = e'$. You will show this in the homework.

Example 1.4. Here's another example based on a group we've seen before. Let $G = S_3$ be the symmetry group on 3 letters. Recall that

$$S_3 = \{\text{bijections } \{1,2,3\} \to \{1,2,3\}.$$

Set $\sigma, \tau \in S_3$ to be the bijections

$$\sigma = \begin{pmatrix} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{pmatrix}.$$

To check that $\sigma\tau = \sigma \circ \tau \neq \tau \circ \sigma = \tau\sigma$, let's check what they do to the element 1. We have[2]

$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(2) = 3,$$
$$(\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(1) = 2.$$

Definition 1.5. A group G is called **abelian** if $m(g,h) = m(h,g)$ for all h and g. Otherwise, G is called **non-abelian**.

As we have seen, S_3 is not abelian, and S_n for $n \geq 3$ is also not abelian.

1.2 More examples of groups

Example 1.6. Let $G = \{\mathbb{O}, \mathbb{E}\}$. Let $m : G \times G \to G$ be

$$(\mathbb{E},\mathbb{E}) \mapsto \mathbb{E}, \quad (\mathbb{E},\mathbb{O}) \mapsto \mathbb{O}, \quad (\mathbb{O},\mathbb{E}) \mapsto \mathbb{O}, \quad (\mathbb{O},\mathbb{O}) \mapsto \mathbb{E}.$$

This operation is some fuzzy-wuzzy way of adding numbers, even and odd. It seems like $\mathbb{E}$ is the identity, the inverses of $\mathbb{E}, \mathbb{O}$ are $\mathbb{E}, \mathbb{O}$ respectively, and you have to check associativity.

Definition 1.7. Given a group G, the **order** of G is the number of elements G, and it is denoted by $|G|$.

So far, we've seen three groups of order 2:

- $G = \{\mathbb{O}, \mathbb{E}\}$
- $G = \{\pm 1\}$ under multiplication
- S_2

You'll prove that all three are isomorphic. In fact, all groups of order 2 are isomorphic!

How would you ever prove that? You can encode the structure of a group in a multiplication table. If G is a group, its **multiplication table** is a $|G| \times |G|$ chart that looks like Table 1. On the top row and left column, you write down the elements of G, and in the entries you write down the products of the elements.

m	$\cdots$	g	$\cdots$
$\vdots$			
h		$m(h,g) = hg$	
$\vdots$			

Table 1: A multiplication table

	$\mathbb{E}$	$\mathbb{O}$
$\mathbb{E}$	$\mathbb{E}$	$\mathbb{O}$
$\mathbb{O}$	$\mathbb{O}$	$\mathbb{E}$

	1	-1
1	1	-1
-1	-1	1

Table 2: Multiplication tables of $G = \{\mathbb{O}, \mathbb{E}\}$ and $G = \{\pm 1\}$

For example, the multiplications of $G = \{\mathbb{O}, \mathbb{E}\}$ and $G = \{\pm 1\}$ are as in Table 2. They look the same, and this means that they are isomorphic.

Recall that a number N is odd if it can be written as $N = 2k + 1$, and even if it can be written as $N = 2k$. We can generalize this. Fix a positive integer $n > 0$. Then given a number N, we have the cases

$$N = \begin{cases} an, & \text{(i.e., } n \text{ divides } N\text{)} \\ an + 1, & \\ \vdots & \\ an + (n-1). & \end{cases}$$

Definition 1.8. Given $N \in \mathbb{Z}$, the unique number $0 \leq b \leq n - 1$ such that

$$N = an + b, \quad a \in \mathbb{Z}$$

is called N mod n. (In this old school, b is called the **remainder** of N/n.)

Definition 1.9. The group $\mathbb{Z}/n\mathbb{Z}$ (the reason for the notation will be clear soon.) is the set $\{0, 1, \ldots, n-1\}$ with group operation as follows:

$$m(a, b) = (a + b) \bmod n.$$

I want to show you another example. There is a mattress on the floor, and I've posted a yellow paper one corner of the mattress. Now we will look at ways to move it around and be at the same position. This is going to be a group, and it is called the "mattress group". We can rotate the mattress around 180 degrees about the x, y, z axes. I'm going to call them R_x, R_y, and R_z.

But you might be able to compose some of these rotations and get some new action. (Here we're exploring the concept of generators and relations.) So

[2]There is a notational convention on arrows. If $f : I \to J$ is a function, with I and J be sets, I just use arrows like $\to$. But if I want to denote where elements are mapped to, I use an arrow with a vertical arrow like $i \mapsto f(i)$.

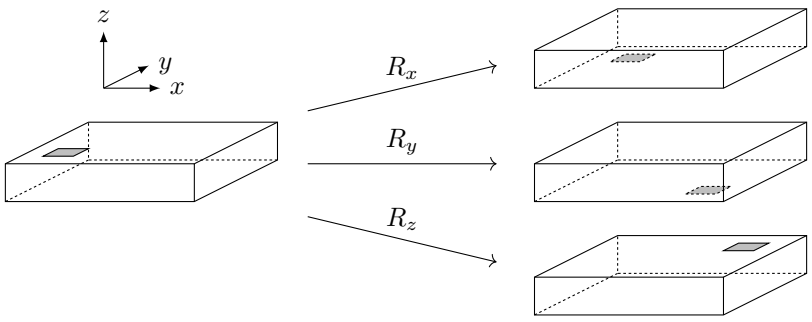


Figure 1: Rotating the mattress about the axes

let's compose some of these. Because by rotating 360 degrees is doing nothing, we see that the diagonal of the multiplication table is all e's. You can see that $R_y R_x = R_z$ by actually rotating the mattress. Then we use a trick that each column or row has to contain all group elements exactly once, like Sudoku. (Here I'm slightly cheating because we haven't shown that e, R_x, R_y, R_z are all the group elements.) Then you can fill out the entire table. You can easily see that this group is abelian, because the table is symmetric about the diagonal.

	e	R_x	R_y	R_z
e	e	R_x	R_y	R_z
R_x	R_x	e	R_z	R_y
R_y	R_y	R_z	e	R_x
R_z	R_z	R_y	R_x	e

Table 3: Multiplication table of the mattress group

2 September 6, 2017

I'm going to give you two exercises.

Exercise 2.1. Let G be a group.

(a) Show that, for every $g, h \in G$,

$$(gh)^{-1} = h^{-1}g^{-1}.$$

(b) Set $g^0 = e$, $g^a = g \cdot \cdots \cdot g$ multiplied a times if $a > 0$, and $g^a = g^{-1} \cdot \cdots \cdot g^{-1}$ multiplied $-a$ times if $a < 0$. Show that $g^{a+b} = g^a g^b$.

You'll need these to submit a correct answer for a problem in the problem set. I'll give you five minutes to try.

Solution. (a) We have

$$h^{-1}g^{-1}(gh) = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$$

by associativity. You can similarly check $gh(h^{-1}g^{-1}) = e$. This shows that $h^{-1}g^{-1}$ is the inverse of gh. In fact, you'll show that this inverse is unique.

(b) If a and b have the same sign, we can do this by associativity. For instance, if $a, b > 0$, then

$$g^{a+b} = \overbrace{g \cdot \cdots \cdot g}^{a+b} = \overbrace{g \cdot \cdots \cdot g}^{a} \cdot \overbrace{g \cdot \cdots \cdot g}^{b} = g^a g^b.$$

If they have different signs, say $a < 0$ and $b > 0$ and $|a| > |b|$ so $a + b < 0$, then

$$g^a g^b = (\overbrace{g^{-1} \cdots g^{-1}}^{|a|})(\overbrace{g \cdots g}^{|b|}) = \overbrace{g^{-1} \cdots g^{-1}}^{|a+b|} = g^{a+b}.$$

You can check other cases similarly. □

Corollary 2.2. *For every $g \in G$, define the map*

$$\phi_g : \mathbb{Z} \to G; \quad a \mapsto g^a.$$

Then ϕ_g is a homomorphism.

Note that $\phi_g(1) = g$.

2.1 Subgroups

Now we come to a notion you might have already thought about.

Definition 2.3. Let G be a group. A subset $H \subseteq G$ is called a **subgroup** if ....

This notion, whatever it is, should be a subset. It should also be a group under "the same operation". But the point of mathematics is to have precise statements.

Definition 2.4. Let G be a group. A subset $H \subseteq G$ is called a **subgroup** if

(1) $e \in H$,
(2) $h^{-1} \in H$ for all $h \in H$ ("closure under inverses")
(3) $h_1 h_2 \in H$ for all $h_1, h_2 \in H$ ("closure under multiplication").

The reason this works is the following. When H is a subgroup, we can take the multiplication from G and define

$$m_H : H \times H \to H; \quad (h_1, h_2) \mapsto m(h_1, h_2).$$

Then (H, m_H) is a group.

Example 2.5. For G a group and $g \in G$, let

$$\langle g \rangle = \{e, g^{\pm 1}, g^{\pm 2}, \ldots\} = \bigcup_{n \in \mathbb{Z}} \{g^n\} = \{g^n : g \in \mathbb{Z}\}.$$

This is a subgroup of G, an is called the **subgroup of G generated by g.**

Example 2.6. Let $G = (\mathbb{C} \setminus \{0\}, \times)$. This is a group since for any $z \in \mathbb{C} \setminus \{0\}$, there is an inverse

$$z^{-1} = \frac{\bar{z}}{\|z\|^2}.$$

Let

$$H = S^1 = \{z : \|z\| = 1\}.$$

Then $\|z\| = 1$ implies $\|z^{-1}\| = \|\bar{z}\|/\|z\|^2 = 1$. Also, $\|z_1\| = \|z_2\| = 1$ implies $\|z_1 z_2\| = \|z_1\|\|z_2\| = 1$. This shows that H is a subgroup.

2.2 Group actions

Remember I introduced groups as symmetries of some kind. So a group should "do" something to a thing.

Definition 2.7. Let G be a group and X be a set. A **(left) group action** of G on X is a function

$$\mu : G \times X \to X; \quad (g, x) \mapsto \mu(g, x) = gx$$

such that

(1) $ex = x$ (i.e., $\mu(e, x) = x$ for all $x \in X$),
(2) $(gh)x = g(hx)$ for all $g, h \in G$ and $x \in X$.

This may seem like an abstract definition, but here is an example.

Example 2.8. Let $X = \mathbb{C}$ be the all of complex numbers, and let $G = S^1$. Rotation is a function given by

$$S^1 \times \mathbb{C} \to \mathbb{C}; \quad (e^{i\theta}, x) \mapsto e^{i\theta}x.$$

You can easily check that $1 \cdot x = x$ and $(e^{i(\theta_1+\theta_2)})x = e^{i\theta_1}(e^{i\theta_2}x)$.

Example 2.9. Let $H \subseteq G$ be a subgroup. Consider the function

$$\mu : H \times G \to G; \quad (h, g) \mapsto hg = m_G(h, g).$$

This is a left group action of H on $X = G$.

Example 2.10. Let $X = \mathbb{R}^2$, and

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right\}.$$

(This group G is the subgroup of $\mathrm{GL}_2(\mathbb{R})$, the group of invertible 2×2 matrices.) The action is given by multiplying matrices:

$$G \times \mathbb{R}^2 \to \mathbb{R}^2; \quad \left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right) \mapsto \begin{pmatrix} x_1 + ax_2 \\ x_2 \end{pmatrix}.$$

The line $x_2 = 0$ is fixed, but the lines $x_2 = a$ are shifted either right of left. This is some sheering action.

Definition 2.11. Let G be a group and X be a set. A **(right) group action** of G on X is a function

$$X \xleftarrow{\mu} X \times G$$

such that $xe = \mu(x, e) = x$ and $x(gh) = (xg)h$.

This looks really stupid, but it can be a useful notion.

Example 2.12. Let $H \subseteq G$. Then

$$G \leftarrow G \times H; \quad gh_{\hookleftarrow}(g, h)$$

is a *right* action of H on G. If G is not abelian, then the left action and the right action look completely different.

Here is an abstraction you may or may not like. Let

$$\mathrm{Aut}_{\mathsf{Set}}(X) = \{\text{bijections } X \to X\},$$

which is a group. Then a **left group action** of G on X is the same thing as a group homomorphism

$$G \to \mathrm{Aut}_{\mathsf{Set}}(X); \quad e \mapsto (x \mapsto x), \quad g \mapsto (x \mapsto gx).$$

However, a **right action** of G is a group homomorphism

$$G^{\mathrm{op}} \to \mathrm{Aut}_{\mathsf{Set}}(X),$$

where G^{op} is a group you can define as (G, m^{op}) and $m^{\mathrm{op}}(g, h) = m(h, g)$.

Definition 2.13. Let $\mu : G \times X \to X$ be a G-action on X. Then for $x \in X$, the **orbit** of x is the set

$$\mathcal{O}_x = \{gx : g \in G\}.$$

Example 2.14. In the case $G = S^1$ and $X = \mathbb{C}$, the orbit of x is the set of complex numbers having the same norm as x.

3 September 11, 2017

Exercise 3.1. Let $\phi : G \to K$ be a group homomorphism. Show that

$$G \times K \to K; \quad (g, k) \mapsto \phi(g)k$$

defines a (left) group action of G on K.

Exercise 3.2. Show that putting an equivalence relation on X is the same thing as writing X as a disjoint union or subsets.

This second exercise explains what equivalence relations are without the formalism from last class. Consider the circle S^1 acting on $\mathbb{C}$ for instance. The action gives an equivalence relation, and this partitions $\mathbb{C}$ into orbits, namely concentric circles.

Solution to Exercise 3.1. We check that

$$(e_G, k) \mapsto \phi(e_G)k = e_K k = k$$

and

$$(gh, k) \mapsto (\phi(gh))k = (\phi(g)\phi(h))k = \phi(g)(\phi(h)k) = g(h \cdot k). \qquad \square$$

Solution to Exercise 3.2. Recall that an equivalence relation defines equivalence classes:

$$x \in [x] : \{y \in X : y \sim x\}.$$

Every element is in some equivalence class, and any two equivalence class are either the same or disjoint. So $\coprod [x] = X$. $\square$

Here is a useful construction. Fix a group action

$$G \times X \to X; \quad (g, x) \mapsto gx.$$

Consider the **set of orbits** $G \setminus X$ of this action.

Example 3.3. As before, set $G = S^1$ and $X = \mathbb{C}$. There is an orbit for every $r \in \mathbb{R}_{\geq 0}$, i.e., there is a bijection

$$S^1 \setminus \mathbb{C} \to \mathbb{R}_{\geq 0},$$

with the equivalence class $[z] = \mathcal{O}_z = \{z' : \|z'\| = \|z\|\}$ sent to $\|z\|$.

Example 3.4. Fix $N \in \mathbb{Z}$, and let $G = \mathbb{Z}$. (Actually take $N = 5$.) Consider the subgroup $H = \{0, \pm N, \pm 2N, \ldots\}$. This induces the action

$$G \times H \to G; \quad (a, b) \mapsto a + b.$$

The orbits is going to be

$$\mathbb{Z}/N\mathbb{Z} \cong \{0, 1, \ldots, N-1\},$$

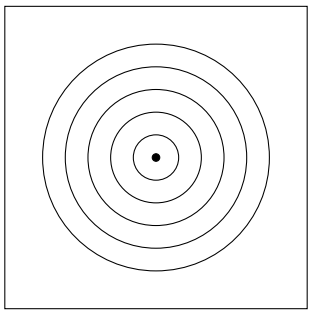


Figure 2: Orbits of $S^1 \curvearrowright \mathbb{C}$

or explicitly

$$\begin{aligned}\mathbb{Z}/N\mathbb{Z} = \{&\mathcal{O}_0 = \{0, \pm N, \pm 2N, \ldots\},\\ &\mathcal{O}_1 = \{1, 1 \pm N, 1 \pm 2N, \ldots, \},\\ &\vdots\\ &\mathcal{O}_{N-1} = \{N-1, N-1 \pm N, N-1 \pm 2N, \ldots\}\}.\end{aligned}$$

3.1 Cosets

Definition 3.5. Let $H \subseteq G$ be a subgroup. Then for any $g \in G$, let

$$\begin{aligned}gH &= \{g' \in G : g' = gh \text{ for some } h \in H\}\\ &= \mathcal{O}_g \text{ under the right group action } G \times H \to G.\end{aligned}$$

Exercise 3.6. Show that $g_1H = g_2H$ if and only if $g_2^{-1}g_1 \in H$.

Solution. For the inverse direction, let's show that $g_1H \subseteq g_2H$ and also $g_2H \subseteq g_1H$. Suppose that $g' \in g_1H$. Then by definition, $g' = g_1h$ for some $h \in H$. Because $g_2^{-1}g_1 \in H$,

$$g' = g_1h = g_1(g_1^{-1}g_2)(g_2^{-1}g_1h) = g_2(g_2^{-1}g_1h) \in g_2H.$$

This shows that $g_1H \subseteq g_2H$ and the other inclusion $h_2H \subseteq g_1H$ can be proven similarly.

For the forward direction, assume that $g_1H = g_2H$. For an arbitrary element $g' = g_1h \in g_1H$, it can be expressed as $g' = g_2h'$ since it is in g_2H. So $g_1h = g_2h'$. This implies

$$g_2^{-1}g_1 = h'h^{-1} \in H. \qquad \square$$

Definition 3.7. This set gH is called the **(left) coset** of H in G with respect to g.

3.2 Toward quotient groups

In class I defined a group structure on $\{0, 1, \ldots, N-1\}$ by $m(a, b) = a+b \bmod N$. This is a group that clearly inherits the group structure from $\mathbb{Z}$. On the other hand, I have define $\mathbb{Z}/N\mathbb{Z}$, which came from $\mathbb{Z}$, but we didn't have a group structure here.

Question. *Does the set G/H inherit a group structure from G? In particular, when does the function*

$$G/H \times G/H \to G/H; \quad (g_1H, g_2H) \mapsto g_1g_2H$$

make G/H a group?

This is actually a trick question. The above all works out nicely if H satisfies some good condition, and try to find out this condition.

4 September 13, 2017

I am not happy with the way I was taught about orbits.

4.1 Another definition of orbits

Fix a group action $G \times X \to X$.

Definition 4.1. A subset $I \subseteq X$ is called an **orbit** (of this action) if the following three properties are satisfied:

(1) $I \neq \emptyset$

(2) for every $y_1, y_2 \in I$, there exists a $g \in G$ such that $gy_1 = y_2$

(3) for every $y \in I$ and $g \in G$, $gy \in I$.

I like this definition more than the $\mathcal{O}_x$ definition, because notation $\mathcal{O}_x$ makes it seem something that depends on x. So in an orbit, there actually is no preferenced element.

Proposition 4.2. *Let I be an orbit. Then for each $x \in I$, actually $I = \mathcal{O}_x$.*

Proof. Let's show that $I \subseteq \mathcal{O}_x$ and $\mathcal{O}_x \subseteq I$. We have $I \subseteq \mathcal{O}_x$ by (2), since $y \in I$ and $y = gx$ implies $y \in I$. On the other hand, $\mathcal{O}_x \subseteq I$ follows from (3). □

Corollary 4.3. *Let $G \times X \to X$ be a group action.*

(i) Every $x \in X$ is contained in some orbit, namely $\mathcal{O}_x$.

(ii) If I, J are orbits, either $I \cap J \neq \emptyset$ or $I = J$.

(iii) $\mathcal{O}_x = \mathcal{O}_y$ if and only if there exists a $g \in G$ such that $gx = y$.

4.2 Normal subgroup

Let's get back to this trick question.

Question. *When does a subgroup H have the property that*

$$G/H \times G/H \to G/H; \quad (g_1H, g_2H) \mapsto (g_1g_2)H$$

makes G/H into a group?

Let me give you a stupid false proof.

False proof. The element $eH \in G/H$ is the identity. We check that

$$gH \cdot eH = geH = gH, \quad eH \cdot gH = egH = gH.$$

Well, we also see that $g^{-1}H$ is the inverse of gH, because

$$(g^{-1}H)(gH) = (g^{-1}g)H = eH, \quad gH \cdot (g^{-1}H) = (gg^{-1})H = eH.$$

Finally, associative holds because

$$(g_1H \cdot g_2H)(g_3H) = (g_1g_2H)g_3H = (g_1g_2)g_3H = g_1(g_2g_3)H = g_1H(g_2H \cdot g_3H).$$

So G/H is always a group. □

The problem is that we don't even know that this is a function. By writing an element of G/H as g_1H, we are assuming that g_1 is the preferred element of the set g_1H. Let me be more explicit.

Problem. *Suppose $g_1'H = g_1H$ and $g_2'H = g_2H$. Does $g_1g_2H = g_1'g_2'H$?*

I'll give you some time to think about this. If G were abelian, then this is always true. This was a great insight. If H were the trivial subgroup, then orbits consist of one elements, and this is also great insight.

Proposition 4.4. *Suppose H satisfies the property that for every $g \in G$,*

$$H = gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

Then the Problem above has an affirmative answer.

Proof. Just to simplify things, assume that $g_2' = g_2$. (You can try to work out the full proof.) Note that $g_1'H = g_1H$ means that $g_1' = g_1h_1$ for some $h_1 \in H$. Likewise, to show that $g_1'g_2H = g_1g_2H$, we want to show that for $h \in H$, $g_1'g_2h \in g_1g_2H$.

Since $g_1' = g_1h_1$, we can write

$$g_1'g_2h = g_1h_1g_2h.$$

I can win if we can move g_2 to move past h_1. Then I will have g_1g_2 times something in H. Since $H = g_2Hg_2^{-1}$, there exists some h_2 such that $h_1 = g_2h_2g_2^{-1}$. Then

$$g_1'g_2h = g_1h_1g_2h = g_1(g_2h_2g_2^{-1})h = g_1g_2h_2h \in g_1g_2H.$$

So I win. □

Definition 4.5. A subgroup $H \subseteq H$ is called **normal** (in G) if for every $g \in G$,

$$gHg^{-1} = H.$$

A cautionary remark: a subgroup H being normal is a property that is relative to G.

Exercise 4.6. Let G be abelian. Then for every subgroup $H \subseteq G$ and $g \in G$, we have $gHg^{-1} = H$.

Exercise 4.7. Let G be any group and let $H = \{e_G\}$. Then for every $g \in G$, we have $gHg^{-1} = H$.

4.3 Quotient groups

Theorem 4.8. *If H is a normal subgroup of G, then*

$$G/H \times G/H \to G/H; \quad (g_1H, g_2H) \mapsto (g_1g_2)H$$

makes G/H into a group.

Note that there exists a function

$$q : G \to G/H; \quad g \mapsto gH,$$

and this is a group homomorphism.

Proof. I need to show that q respects multiplication. We check

$$q(g_1g_2) = (g_1g_2)H = g_1H \cdot g_2H = q(g_1)q(g_2). \qquad \square$$

This process of quotienting by H needs to be collapsing by H. Let me make this formal.

Proposition 4.9. $q^{-1}(e_{G/H}) = H$.

Proof. Just check

$$q^{-1}(e_{G/H}) = \{g \in G : q(g) = e_{G/H}\} = \{g \in G : q(g) = H\} = H. \qquad \square$$

Sometimes you would want to know what gets collapsed in general.

Definition 4.10. Let $\phi : G \to K$ be a group homomorphism. Then the **kernel** of ϕ, denoted $\ker(\phi)$, is the set $\phi^{-1}(e_K) = \{g \in G : \phi(g) = e_K\}$.

Theorem 4.11. *A subgroup $H \subseteq G$ is normal in G if and only if $H = \ker(\phi)$ for some group homomorphism $\phi : G \to K$.*

5 September 15, 2017

Writing your own solutions is really a important process, so please go through it yourself.

Last time, we talked about a function

$$\pi : G \to G/H; \quad g \mapsto gH$$

where $H \subseteq G$ is a subgroup. This is always well-defined, but a priori it is only a function. More importantly, we had the following theorem.

Definition 5.1. A subgroup $H \subseteq G$ is called **normal** in G when $gHg^{-1} = H$ for all $g \in G$.

Theorem 5.2. *Assume that H is normal in G. Then the function*

$$G/H \times G/H \to G/H; \quad (g_1H, g_2H) \mapsto g_1g_2H$$

is well-defined, and makes G/H a group.

When H is normal, we write $H \lhd G$, and the group G/H is called the **quotient group**.

Proof. Let's prove that the function is well-define.d We need to show that if $g_1H = g_1'H$ and $g_2H = g_2'H$ then $g_1g_2H = g_1'g_2'H$. The conditions are equivalent to that there exist h_1 and h_2 such that

$$g_1 = g_1'h_1, \quad g_2 = g_2'h_2.$$

Now we want to show that

$$g_1g_2 = (g_1'h_1)(g_2'h_2)$$

can be written as $g_1'g_2'$ times something in H. Since $H \lhd G$, there exists some h_1' such that

$$h_1 = g_2'h_1'(g_2')^{-1}.$$

Then we can write

$$g_1g_2 = (g_1'h_1)(g_2'h_2) = g_1'(g_2'h_1'(g_2')^{-1})g_2'h_2 = g_1'g_2'h_1'h_2.$$

Here $h_1'h_2 \in H$, and so $g_1g_2H = g_1'g_2'H$. □

5.1 Kernel and image

Definition 5.3. Fix a group homomorphism $\phi : G \to L$. The **kernel** of ϕ is the set

$$\ker(\phi) = \{g \in G : \phi(g) = e_L\}.$$

This actually extends the notion of a kernel in the context of vector spaces. Note that a vector space is always a group.

Exercise 5.4. Fix a group homomorphism $\phi : G \to L$. Prove that ϕ is an injection if and only if $\ker(\phi) = \{e_G\}$.

Solution. For the forward direction, assume that ϕ is an injection. This means that $\phi(g_1) = \phi(g_2)$ implies $g_1 = g_2$. We know that $\phi(e_G) = e_L$, so $g_1 \in \ker\phi$ or $\phi(g_1) = e_L$ implies $g_1 = e_L$. That is, $\ker\phi = \{e_G\}$.

Now suppose that $\ker\phi = \{e_G\}$. Take any $g_1, g_2 \in G$ with $\phi(g_1) = \phi(g_2)$. Then $\phi(g_2)^{-1}\phi(g_1) = e_L$. Because ϕ is a homomorphism, we have $\phi(g_2^{-1}g_1) = e_L$. Then $g_2^{-1}g_1 \in \ker\phi$ and so $g_2^{-1} = g_1$. This means that $g_1 = g_2$. □

Definition 5.5. Fix $\phi : G \to L$ a group homomorphism. Then the **image** of ϕ is

$$\mathrm{im}(\phi) : \{\ell \in L : \ell = \phi(g) \text{ for some } g \in G\}.$$

Exercise 5.6. (1) $\mathrm{im}(\phi) \subseteq L$ is a subgroup.

(2) $\ker(\phi) \subseteq G$ is a subgroup.

(3) $\ker(\phi) \lhd G$ is actually a normal subgroup.

Solution. (1) We need to show that $e_L \in \mathrm{im}\,\phi$, it is closed under inverses, and that it is closed under multiplication. Clearly $e_L \in \mathrm{im}\,\phi$ because $\phi(e_G) = e_L$. If $\ell = \phi(g)$, then $\ell^{-1} = \phi(g)^{-1} = \phi(g^{-1})$. If $\ell_i = \phi(g_i)$, then $\ell_1\ell_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2)$. This shows that $\mathrm{im}\,\phi$ is a subgroup of L.

(2) Likewise we check that $e_G \in \ker\phi$. If $g \in \ker\phi$, then $\phi(g) = e_L$ and so $\phi(g^{-1}) = \phi(g)^{-1} = e_L$. If $g_1, g_2 \in \ker\phi$, then $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = e_Le_L = e_L$.

(3) Fix $g \in G$ and $k \in \ker\phi$. We need to show that $gkg^{-1} \in \ker\phi$, i.e., $\phi(gkg^{-1}) = e_L$. But we have

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e_L.$$

This shows that $\ker(\phi)$ is a normal subgroup. □

Note that any subgroup $L' \subseteq L$ is the image of some homomorphism. There is a function called "include":

$$L' \to L; \quad \ell \mapsto \ell.$$

5.2 Universal property of quotient groups

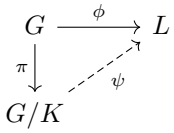
Now that you know kernels, images, and quotient groups, you have a plethora of ways to construct all kinds of new groups. Whenever you have a homomorphism, you can construct groups.

Theorem 5.7 (First isomorphism theorem)**.** *Fix a group homomorphism $\phi : G \to L$. Then there exists a natural isomorphism*

$$G/\ker(\phi) \to \mathrm{im}(\phi).$$

It is not even clear if you can construct this function. God gave you the map $G \to L$ at the beginning of this theorem, and this theorem says that we can actually construct this mysterious map $G/\ker\phi \to \operatorname{im}\phi$.

Theorem 5.8 (Universal property for quotient groups)**.** *Fix $\phi : G \to L$ a group homomorphism. Assume $K \subseteq G$ is a subgroup such that $K \subseteq \ker\phi$. There is a function $\pi : G \to G/K$. Then there exists a unique function $\phi : G/K \to L$ such that $\psi \circ \pi = \phi$.*



Moreover, if $K \lhd G$, then ψ is a group homomorphism.

Example 5.9. Let $G = \mathbb{Z}$ and L be whatever, say $\mathbb{C}$. Now let $\phi : \mathbb{Z} \to \mathbb{C}$ be a map with nonzero kernel. Then the theorem says that ϕ actually factors through $\mathbb{Z}/\ker\phi = \mathbb{Z}/n\mathbb{Z}$ for some n. So ϕ actually doesn't care much about the elements themselves; it only cares about its remainder mod n.

Proof. Note that if ψ exists, ψ has to be unique because π is a surjection. So let's show that it exists. Define ψ to be

$$\psi : G/K \to L; \quad gK \mapsto \phi(g).$$

We just need to show that this function is well-defined. If $g_1K = g_2K$, then $g_1 = g_2k$ for $k \in K$. So

$$\phi(g_1) = \phi(g_2k) = \phi(g_2)\phi(k) = \phi(g_2)e_L = \phi(g_2).$$

This means that the map ψ is well-defined, and it clearly satisfies $\psi \circ \pi = \phi$.

When $K \lhd G$, we need to show that $\psi(g_1K \cdot g_2K) = \psi(g_1K)\psi(g_2K)$. But when the product for cosets is defined as

$$\psi(g_1K \cdot g_2K) = \psi(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \psi(g_1K)\psi(g_2K).$$

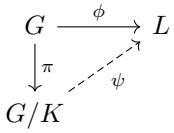
This shows that ψ is indeed a group homomorphism. □

6 September 18, 2017

Last time, we fixed a group homomorphism $\phi : G \to L$, and defined the image and kernel as

$$\begin{aligned} \operatorname{im}(\phi) &= \{\ell \in L : \ell = \phi(g) \text{ for some } g \in G\} \subseteq L, \\ \ker(\phi) &= \{g \in G : \phi(g) = e_L\} \lhd G. \end{aligned}$$

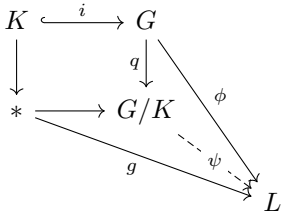
Theorem 6.1. *Fix $\phi : G \to L$. Suppose $K \subseteq G$ is a subgroup that is contained in $\ker(\phi)$. Then there exists a unique function $\psi : G/K \to L$ such that $\psi \circ \pi = \phi$.*



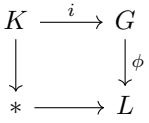
Moreover, if $K \lhd G$, then ψ is a group homomorphism.

The reason we could define ψ was that $\psi(gK) = \phi(g)$ made sense because K is contained in the kernel. There is another formulation of the universal property of quotient groups.

Theorem 6.2 (Universal property of quotient groups)**.** *Suppose $K \lhd G$. Fix a group homomorphism $\phi : G \to L$ and assume that $\ker(\phi) \supseteq K$. (This means that the composition $K \hookrightarrow G \to L$ is trivial, i.e., that $K \hookrightarrow G \to L$ and $K \to * \to L$ are equal.) Then there exists a unique group homomorphism $\psi : G/K \to L$ such that $\phi = \varphi \circ \pi$.*



If you think hard, you will notice that asserting that the diagram

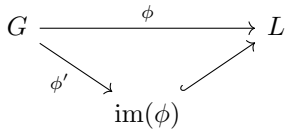


commutes is just another way of asserting that $K \subseteq \ker(\phi)$. This is also why the square consisting of $K \to G \to G/K$ and $K \to * \to G/K$ commutes.

Why would anyone try to draw such a diagram which looks like a total mess? You could always try to draw this diagram where the algebraic objects are different. For instance, you can consider these diagrams that have sets and functions, vector spaces and linear transformations, rings and ring homomorphisms, or modules and linear morphisms.

6.1 The first isomorphism theorem

Note that any map always factors through the image $\mathrm{im}(\phi)$.



Theorem 6.3 (First isomorphism theorem)**.** *Fix $\phi : G \to L$ a group homomorphism. Then the group homomorphism*

$$G/\ker(\phi) \to \mathrm{im}(\phi)$$

is an isomorphism.

Proof. First, we check that this is a homomorphism by the universal property. (This is the same as doing $\psi(g\ker(\phi)) = \phi(g)$ all over again.) To show that this map is an injection, it suffices to show that

$$\ker(\psi) = \{e_{G/\ker(\phi)}\} = \{\ker\phi\}.$$

But we can compute

$$\ker(\psi) = \{g\ker\phi : \psi(g\ker\phi) = e_L\} = \{g\ker\phi : \phi(g) = e_L\} = \{\ker\phi\}.$$

We finally need to show that $\psi : G/\ker(\phi) \to \mathrm{im}(\phi)$ is a surjection. Note that $\ell \in \mathrm{im}(\phi)$ is equivalent to there being a $g \in G$ such that $\phi(g) = \ell$. This is in tern equivalent to there being a $g \in G$ such that

$$\psi(g\ker(\phi)) = \phi(g) = \ell.$$

That is, the image of ψ is indeed the whole of $\mathrm{im}(\phi)$. □

6.2 Subgroups generated by an element

These applications are math applications, not applications to the real world. Our goal is to study subgroups of an arbitrary group. We can look at one element, multiply with itself and get a subgroup. We define

$$\langle g\rangle = \{\ldots, (g^{-1})^2, g^{-1}, e, g, g^2, \ldots\} = \{g^a\}_{a\in\mathbb{Z}}.$$

Definition 6.4. We let $\langle g\rangle = \{g^a\}_{a\in\mathbb{Z}}$ and call it the **subgroup of G generated by g.**

Exercise 6.5. Given any $g \in G$, show that there exists an isomorphism

$$\langle g\rangle \cong \mathbb{Z}/n\mathbb{Z}$$

for some $n \geq 0$. (Here note that $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.)

Solution. Recall that there is a group homomorphism

$$\phi_\gamma : \mathbb{Z} \to G; \quad a \mapsto g^a.$$

Note that $\mathrm{im}(\phi_g)$ is just the set of elements that can be written as g^a for some a. This is by definition $\langle g \rangle$. On the other hand, by the first isomorphism theorem,

$$\mathrm{im}(\phi_g) \cong \mathbb{Z}/\ker(\phi_g).$$

By Homework, any subgroup of $\mathbb{Z}$ is equal to the set $n\mathbb{Z}$ for some $n \geq 0$. So $\ker(\phi_g) = n\mathbb{Z}$ for some $n \geq 0$. In other words,

$$\langle g \rangle = \mathrm{im}(\phi_g) \cong \mathbb{Z}/\ker(\phi_g) = \mathbb{Z}/n\mathbb{Z}. \qquad \square$$

This number n then looks like a pretty cool invariant of the element $g \in G$.

Proposition 6.6. *Fix $g \in G$, and some (finite) integer $n > 0$. Then the following are equivalent:*

(i) $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$,

(ii) *n is the smallest positive integer such that $g^n = e_G$,*

(iii) $\ker(\phi_g) = n\mathbb{Z}$.

Assuming this proposition, we can make a definition

Definition 6.7. If such $n > 0$ exists, n is called the **order** of G. On the other hand, if $\langle g \rangle \cong \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$, then the order of g is called "infinite". We denote the order of g by $|g|$.

Example 6.8. In Homework you showed if $|G| < \infty$ and $H \subseteq G$ is a subgroup, then $|H|$ divides $|G|$. So $|\langle g \rangle|$ divides $|G|$. That is, the order of any element of a finite group divides the order of the group.[3]

Example 6.9. Let $G = S_3$ so that $|G| = 6$. Then there is no $g \in G$ such that $|g| = 4$.

Definition 6.10. Let G be a group. If there exists a $g \in G$ such that $\langle g \rangle = G$, then G is called a **cyclic group**.

Corollary 6.11. *Any cyclic group G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 0$.*

Exercise 6.12. Let G be a group of order p, where p is a prime number. Then G isomorphic to any other group of order p.

Solution. Choose $g \in G$ such that $g \neq e_G$. Then $|g| \geq 2$ because $\{e_G, g\} \subseteq \langle g \rangle$. On the other hand, $|g|$ divides $|G| = p$. Because $|g| \geq 2$ and p is a prime, we obtain $|g| = p$. That is, $|\langle g \rangle| = p = |G|$ and so $\langle g \rangle = G$. Therefore G is cyclic and

$$G = \langle g \rangle \cong \mathbb{Z}/p\mathbb{Z}$$

by the first isomorphism theorem. $\square$

We'll keep exploring more of these finite groups.

[3] Recall that the order of a group is the number of elements.

7 September 20, 2017

Last time we talked about more quotient stuff. We also talked about order of an element. Give a $g \in G$, there is the subgroup $\langle g \rangle \subseteq G$ generated by g. The order of g is defined as $|g| = |\langle g \rangle|$, which is also the smallest $n > 0$ such that $g^n = e$.

7.1 The dihedral group

Example 7.1. Let us look at the symmetries of a regular n-gon. I can look at the ways I can move the pentagon around and fit it to the same place. (This is like the mattress group.) There is the identity element that does nothing. We could always rotate by $(360/n)^\circ$ or $(720/n)^\circ$ or something counterclockwise. Then

$$\{\text{The rotational symmetries of regular } n\text{-gon}\} \cong \mathbb{Z}/n\mathbb{Z}.$$

This is because it is generated by rotation by $(360/n)^\circ$. If we denote by r the rotation by $(360/n)^\circ$, we have

$$G = \{\text{Rotational symmetries of regular } n\text{-gon}\} = \{e = r^n, r, r^2, \dots, r^{n-1}\} = \langle r \rangle.$$

This also can be thought of as the subgroup of $\mathrm{GL}_2(\mathbb{R})$ with

$$r = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}.$$

In other words, we have an embedding of G into $\mathrm{GL}_2(\mathbb{R})$. It is moreover a subgroup of the circle S^1.

Example 7.2. But by symmetry, we live in three dimensions! So we could also flip this regular 5-gon. Why don't we combine rotations with flipping? Now that we allow reflections, how many symmetries can there be? We at least know that the number is going to be a multiple of 5. The "group of rotations" is a subgroup of the group of total symmetries. So 5 must divide the group of symmetries.

It turns out that there are 10 symmetries. This is because you can choose 5 places where one vertex goes, and then choose 2 adjacent places where an adjacent vertex goes. This generalizes to n-gons, and there are $2n$ symmetries of the regular n-gon including reflections.

To be more rigorous, we can see that

$$\{\text{Rotations}\} \subseteq \{\text{All symmetries}\}$$

is a subgroup, so $|\{\text{All symmetries}\}|$ is a multiple of $|\{\text{Rotations}\}| = n$. On the other hand, the final configuration only depends on where a vertex and its adjacent vertex. So there are at most $2n$ such symmetries. But there are reflections, so there can't be just n symmetries. This shows that the number of symmetries is $2n$.

There are n possible reflections and n rotations. These add up to $2n$. So every non-rotation is actually a reflection about some axis.

Definition 7.3. The group of symmetries of the regular n-gon is called the **dihedral group** and is written D_{2n}.[4]

Exercise 7.4. Show that D_{2n} is not abelian for $n \geq 3$.

Solution. Let r be the rotation by $2\pi/n$ and let s be the rotation about some line. Then it can be checked that $sr \neq rs$.

Here is another way to check this. Choose and injective group homomorphism

$$\phi : D_{2n} \hookrightarrow \mathrm{GL}_2(\mathbb{R}); \quad r \mapsto \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}, \quad s \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Now you can check that

$$\phi(rs) = \phi(r)\phi(s) \neq \phi(s)\phi(r) = \phi(sr)$$

and because ϕ is injective, conclude that $rs \neq sr$. □

In fact, you can check that

$$r^n = e, \quad srs = r^{-1}, \quad s^2 = e.$$

In terms of matrix, reflection has negative determinant and rotation has positive determinant, so srs has to be a rotation.

We can also ask the following question: Suppose you have a group that is generated by r and s, which satisfy these relations. Does this necessarily have to be isomorphic to the dihedral group? The answer is yes, but it is a very subtle question.

7.2 Generators and relations

One way to give/define/present a group is to define a collection of **generators** $x, y, z, \ldots$ and a collection of **relations** these generators satisfy. This is a great way to play around with groups, but some of these groups will be provably undecidable. The notation is

$$G = \langle (\text{generators}) \mid (\text{relations}) \rangle.$$

Example 7.5. What is $G = \langle x \rangle$? This is going to be

$$\langle x \rangle = \{x^n\}_{n \in \mathbb{Z}} \cong \mathbb{Z}$$

because we don't have any relations.

Example 7.6. For $k \in \mathbb{Z}_{>0}$, we can also identify the group

$$G = \langle x \mid x^k = e \rangle \cong \mathbb{Z}/k\mathbb{Z}.$$

[4]Sometimes people write this as D_n. This is very confusing if we write D_{16}. I apologize for that, and we are going to stick to our notation D_{2n}.

Example 7.7. What is $G = \langle x, y \rangle$? This is actually not $\mathbb{Z}^2$ and some crazy huge group. In this group $xy \neq yx$ because we don't have this relation. On the other hand, in $\mathbb{Z}^2$ everything commutes. For instance,

$$x^5 y^3 x^{-2} y^2 x^2 y^{19} x^{-122} \in G$$

and there is no way to simply this. This is called the **free group on** 2 **generators**.

Theorem 7.8 (Word problem)**.** *There exist (finite) presentations of groups* $G = \langle (gen) \mid (rel) \rangle$ *such that it is undecidable whether two expressions of the generators are the same elements.*

8 September 22, 2017

Last time we studied the dihedral groups D_{2n} and talked about generators and n-gons. Today we are going to talk about the symmetric group.

8.1 The symmetric group

If you work with finite sets, you will want to understand the symmetry group of finite sets. This is going to be S_n, if the set has n elements.

Definition 8.1. The **symmetric group** is the set

$$S_n = \{\text{biijections } \{1,\dots,n\} \to \{1,\dots,n\}\}$$

with composition.

We can always write ϕ as

$$\phi : 1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 1, \quad 4 \mapsto 5, \quad 5 \mapsto 4.$$

But this is not efficient and painful to write.

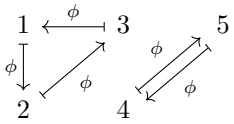
Consider the action

$$S_n \times \{1,\dots,n\} \to \{1,\dots,n\}; \quad (\phi, i) \mapsto \phi(i).$$

This is a group action because $(\phi \circ \phi', i) = \phi(\phi'(i))$. Now $\langle\phi\rangle$ is a subgroup of S_n, and so we get the restriction

$$\langle\phi\rangle \times \{1,\dots,n\} \to \{1,\dots,n\}; \quad (\phi^q, i) \mapsto \phi \circ \cdots \circ \phi(i).$$

We can draw this action as



For any n and $\phi \in S_n$, this element ϕ "breaks up" $\{1,\dots,n\}$ into orbits, called **cycles**. So we have an association

$$\{\text{elements of } S_n\} \quad \longleftrightarrow \quad \left\{ \begin{array}{c} \text{ways to break up} \\ \{a^1 = 1, \phi(1), \phi^2(1), \dots\} \\ \{a^2, \phi(a^2), \phi^2(a^2), \dots\} \\ \vdots \end{array} \right\}.$$

Here, we really have to remember the sequential order of the elements in these orbits. This is because $1 \mapsto 3 \mapsto 2 \mapsto 1$ is different from $1 \mapsto 2 \mapsto 3 \mapsto 1$ although they have the same orbit.

Here, someone could have chosen a different a^2, say $(a^2)'$ but with $(a^2)' \in \mathcal{O}_{a^2}$. So when we remember the ordering, we have to consider the fact that there is a "cyclic" ambiguity.

Example 8.2. ϕ above can be represented as $(1\,2\,3)(5\,4)$, also as $(3\,1\,2)(4\,5)$, and also as $(2\,3\,1)(4\,5)$. But it is not the same as $(1\,3\,2)(5\,4)$.

Definition 8.3. Given an element $\phi \in S_n$, its **cyclic notation** is

$$\phi = (a_1^{(1)}\, a_2^{(1)}\, \cdots\, a_{n_1}^{(1)})(a_1^{(2)}\, a_2^{(2)}\, \cdots\, a_{n_2}^{(2)}) \cdots (a_1^{(k)}\, \cdots\, a_{n_k}^{(k)})$$

such that

- each $a_j^{(i)} \in \{1, \ldots, n\}$,
- $\phi(a_j^{(i)}) = a_{j+1}^{(i)}$ and $\phi(a_{n_i}^{(i)}) = a_1^{(i)}$,
- $\{a_j^{(i)}\} \neq \{a_j^{(i')}\}$ for $i \neq i'$,
- every $a \in \{1, \ldots, n\}$ appears as some $a_j^{(i)}$.

Example 8.4. Let us consider

$$\phi : 1 \mapsto 1, \quad 2 \mapsto 3, \quad 3 \mapsto 2, \quad 4 \mapsto 6, \quad 5 \mapsto 4, \quad 6 \mapsto 5.$$

If we choose 5 as the favorite element, we first get the orbit $(5\,4\,6)$. (Here, $a_1^{(1)} = 5$, $a_2^{(1)} = \phi(a_1^{(1)}) = 4$, $a_3^{(1)} = \phi(a_2^{(1)}) = 6$, and $\phi(a_3^{(1)}) = 5 = a_1^{(1)}$.) Then we can look at other orbits, and write

$$\phi = (5\,4\,6)(1)(3\,2).$$

This can also be written as $\phi = (6\,5\,4)(2\,3)(1)$.

Because we're lazy, we almost always omit one-element cycles. In other words, if a number a does not appear in this cyclic notation, we assume that a is fixed. Then we could write

$$\phi = \mathrm{id}_{\{1,\ldots,n\}} = (1)(2)\cdots(n) = () = e.$$

Exercise 8.5. Write

	1	2	3	4	5	6	7
ϕ	7	6	2	4	1	3	5

in cyclic notation.

Solution. It can be written as $(1\,7\,5)(2\,6\,3)(4)$ or $(1\,7\,5)(2\,6\,3)$ or $(6\,3\,2)(5\,1\,7)$ in many other ways. □

This notation also aids in group multiplication. If $\tau = (1\,2\,3)$ and $\sigma = (3\,4\,5)$ are elements of S_5, then

$$\tau \circ \sigma = (1\,2\,3) \circ (3\,4\,5) = (1\,2\,3\,4\,5).$$

Every element $\phi \in S_n$ determines a cycle, and hence a **cycle shape**

$$\{n_1, n_2, \ldots, n_k\}$$

where order doesn't matter. For example, the cycle shape of $\phi = e = \mathrm{id}_{\{1,\ldots,n\}}$ is $\{1, 1, \ldots, 1\}$ and the cycle shape of $(1\,2\,3)(4\,5) \in S_6$ is $\{3, 2, 1\} = \{1, 3, 2\} = \{1, 2, 3\}$.

So the "cycle shape" of $\phi \in S_n$ is the same thing as a partition of the number n. That is, $n_1 + \cdots + n_k = n$ always.

We now want to study normal subgroups of S_n. I want to know what conjugates of elements look like. It turns out there is a very nice description.

Theorem 8.6. *Two elements $\phi, \phi' \in S_n$ are conjugate, i.e., there exists a $\tau \in S_n$ such that $\phi' = \tau\phi\tau^{-1}$, if and only if ϕ and ϕ' have the same cycle shape.*

9 September 25, 2017

Proposition 9.1. *Given $\phi : G \to L$, $\ker(\phi)$ is normal in G.*

Last time we talked about the symmetric group S_n. Given some $S_n \ni \phi : \{1, \dots, n\} \to \{1, \dots n\}$, we produced a cycle notation:

$$\phi = (a_1^{(1)}, \dots, a_{n_1}^{(1)})(a_1^{(2)}, \dots, a_{n_2}^{(2)}) \cdots (a_1^{(k)}, \dots, a_{n_k}^{(k)}).$$

Theorem 9.2. *$\sigma, \sigma' \in S_n$ are conjugate if and only if σ and σ' have the same cycle shape.*

Definition 9.3. Two element $g, g' \in G$ are **conjugate** if and only if there exists an h such that $hgh^{-1} = g'$.

This is a symmetric notion, because if $hgh^{-1} = g'$, then $(h^{-1})g'(h^{-1})^{-1} = g$.

Definition 9.4. The **cycle shape** of ϕ is the collection of integers $n_1, n_2, \dots, n_k$ without caring about ordering. (Then $n = n_1 + \cdots + n_k$.)

Proof of Theorem 9.2. Let us first prove that same cycle shape implies conjugate. Write

$$\sigma = (a_1^{(1)} \cdots a_{n_1}^{(1)}) \cdots (a_1^{(k)} \cdots a_{n_k}^{(k)}),$$
$$\sigma' = (b_1^{(1)} \cdots b_{n_1}^{(1)}) \cdots (b_1^{(k)} \cdots b_{n_k}^{(k)}).$$

Define $\tau \in S_n$ to be

$$\tau(a_j^{(i)}) = b_j^{(i)}.$$

We claim that τ is the h we seek, i.e., $\tau\sigma\tau^{-1} = \sigma'$. To show this, we check

$$\tau\sigma\tau^{-1}(b_j^{(i)}) = \tau\sigma(a_j^{(i)}) = \tau(a_{j+1}^{(i)}) = b_{j+1}^{(i)} = \sigma'(b_j^{(i)}).$$

Now let us show that conjugate implies same cycle shape. Given τ such that $\tau\sigma\tau^{-1} = \sigma'$, define the sequence $b_j^{(i)}$ by $b_j^{(i)} = \tau(a_j^{(i)})$. Then we claim that

$$(b_1^{(1)} \cdots b_{n_1}^{(1)}) \cdots (b_1^{(k)} \cdots b_{n_k}^{(k)})$$

is a cycle notation for σ'. We can check

$$\sigma'(b_j^{(i)}) = \tau\sigma\tau^{-1}(b_j^{(i)}) = \tau\sigma(a_j^{(i)}) = \tau(a_{j+1}^{(i)}) = b_{j+1}^{(i)}.$$

So σ' has the same cycle shape as σ. □

9.1 Cayley's theorem

Theorem 9.5 (Cayley's theorem)**.** *Let G be a finite group. Then there exists a $n \geq 1$ such that G admits an injective group homomorphism $G \hookrightarrow S_n$.*

This is powerful and philosophically satisfying because everything is inside the symmetric group. This was a theorem a long time ago, but I'm giving as an exercise.

Solution. Let $n = |G|$. G acts on itself by multiplication;

$$G \times G \xrightarrow{\mu = m} G.$$

Choose any bijection $\alpha : G \to \{1, \dots, n\}$. Then any element $g \in G$ gives a bijection

$$\{1, \dots, n\} \xrightarrow{\alpha^{-1}} G \xrightarrow{m(g,-)} G \xrightarrow{\alpha} \{1, \dots, n\}.$$

So we have a function

$$\phi : G \to S_n; \quad g \mapsto \alpha \circ m(g, -) \circ \alpha^{-1}.$$

To show that this is a group homomorphism, we can check that

$$\begin{aligned} \phi(g_1 g_2) &= \alpha \circ m(g_1 g_2, -) \circ \alpha^{-1} = \alpha \circ m(g_1, -) \circ m(g_2, -) \circ \alpha^{-1} \\ &= (\alpha \circ m(g_1, -) \circ \alpha^{-1}) \circ (\alpha \circ m(g_2, -) \circ \alpha^{-1}) = \phi(g_1)\phi(g_2). \end{aligned}$$

Here, $m(g_1 g_2, -) = m(g_1, -) \circ m(g_2, -)$ by associativity.

Now all I need to show that this is homomorphism is an injection. It suffices to show that $\ker(\phi) = \{e_G\}$. But if $\phi(g) = e_{S_n}$, then $gh = h$ for all h. So $g = e_G$. □

So could be why you care about symmetric groups. This theorem is part of the undergraduate curriculum, so this is great. Pedagogically this is also great because we can now talk about normal subgroups.

9.2 More on normal subgroups

Given a group G, what can you do if you want to *force* some element of G to be "equal to e_G"? For instance, consider a group given by generators and relations,

$$H = \langle x, y, z, \dots : (\text{relations}) \rangle.$$

This H is a group obtained from the free group $\langle x, y, z, \dots \rangle$ by imposing relations.

Here is another weird example. Suppose we have the symmetric group $G = S_n$, and we suddenly want to make this abelian, so that $\sigma\tau = \tau\sigma$ for all σ, τ. In other words, we want to $\sigma\tau\sigma^{-1}\tau^{-1} = e_G$.

Recall from an optional problem in Homework 1,

Proposition 9.6. *If $\phi : S_n \to A$ is a group homomorphism to an abelian group A, then $|\phi(S_n)| \leq 2$.*

What does it mean to map to an abelian group? This means that

$$\phi(\sigma\tau) = \phi(\sigma)\phi(\tau) = \phi(\tau)\phi(\sigma) = \phi(\tau\sigma),$$

and so $\phi(\sigma\tau\sigma^{-1}\tau^{-1}) = e_A$. One insight mathematicians have obtained in the last years is that it is possible to understand objects by morphisms out of it.

Definition 9.7. Let G be a group. Given $x, y \in G$, the element $xyx^{-1}y^{-1} \in G$ is called the **commutator** of x and y.

Definition 9.8. The subgroup of G generated by elements of the form $xyx^{-1}y^{-1}$ is called the **commutator subgroup**. This subgroup is written as $[G, G]$.

This is not the subset of commutators. The product of two commutators need not be a commutator.

Proposition 9.9. $[G, G] \lhd G$.

Definition 9.10. Because we have a normal subgroup, we can take the quotient and define $G/[G, G] \cong \mathrm{Ab}(G)$ and call this the **abelianization** of G.

9.3 Sign of a permutation

Example 9.11. What you have proven in the homework is $\mathrm{Ab}(S_n) \cong \mathbb{Z}/2\mathbb{Z}$.

Corollary 9.12. *The group $G = S_n$ has a normal subgroup that is not $\{e_G\}$ or S_n.*

Can anybody thing of a non-trivial homomorphism from $S_n \to \mathbb{Z}/2\mathbb{Z}$? This is the sign homomorphism. Heuristically, this is a homomorphism which sends $(ij) \mapsto 1 \in \mathbb{Z}/2\mathbb{Z}$. This determines the whole homomorphism, because every $\phi \in S_n$ can be written as a composition of transpositions. It is not at all obvious to show that this gives a well-defined homomorphism.

There is another concrete description, if you know about determinants but don't know signs. There is a group homomorphism given by

$$S_n \to \mathrm{GL}_n(\mathbb{R}); \quad \sigma \mapsto (A : e_i \mapsto e_{\sigma(i)}).$$

Then there is a group homomorphism $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$. But it is possible to show that the determinant of any "permutation matrix" is ± 1. So we determine the sign as the composition

$$S_n \to \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$$

and identifying $\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

10 September 27, 2017

10.1 Generated subgroup

Definition 10.1. Let G be a group, and fix a subset $A \subseteq G$. Then the subgroup of G generated by A, $\langle A \rangle$, is...

Here are the proposed definitions:

- $\langle A \rangle$ is the smallest subset of G containing A and closed under multiplication and inverses.
- $\bigcup_{a \in A} \langle a \rangle$
  This not quite what we want, because $(1,0)$ and $(0,1)$ in $\mathbb{Z} \times \mathbb{Z}$ generate the whole group, but individually they generated $\mathbb{Z} \times \{0\}$ and $\{0\} \times \mathbb{Z}$.
- "multiply all a's together"
- $\langle A \rangle$ is the smallest subgroup containing A.

Proposition 10.2. *Let $A, \langle A \rangle \subseteq G$ be subsets. The following are equivalent:*

(1) $\langle A \rangle$ is the smallest non-empty subset of G containing A and closed under multiplication and inverses.

(2) $\langle A \rangle$ is the set of all elements in G that can be written as a product $a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ where $a_i \in A$ and $n_i \in \mathbb{Z}$.

(3) $\langle A \rangle$ is the smallest subgroup containing A.

(4) Let J be the set of all subgroups of G that contain A. Then $\langle A \rangle = \bigcap_{H \in J} H$.

(5) Let $G' = \langle A \mid \text{no relation} \rangle$. Then the assignment $G' \to G$ with $a_1^{n_1} \cdots a_k^{n_k} \mapsto a_1^{n_1} \cdots a_k^{n_k}$ is a group homomorphism and $\langle A \rangle$ is its image.

I'm not going to prove this proposition, but I am going to give some indication.

Lemma 10.3. *Fix subgroups $H, H' \subseteq G$. Then $H \cap H'$ is a subgroup. In fact, for any collection of subgroups, their intersection $\bigcap_{j \in J} H_j$ is also a subgroup.*

Proof. We know that $e_G \in \bigcap_{j \in J} H_j$, because $e_G \in H_j$ for all j. If $h_1, h_2 \in H_j$ for all j, then $h_1 h_2 \in H_j$ for all j. So $h_1 h_2$ is in the intersection. If $h \in H_j$ for all j, then $h^{-1} \in H_j$ for all j and so h^{-1} is in the intersection. □

10.2 Imposing relations

Now I want to do this for quotient groups. To define a group structure on G/H, we need $H \lhd G$.

Often, an element $gH \in G/H$ is just written as $\underline{g}$ or $[g]$. So in this case, $\pi : G \to G/H$ maps $g \mapsto \underline{g}$ or $g \mapsto [g]$. The point of this notation is that mathematicians never thing of elements of G/H as sets. We are identifying $\underline{g} = \underline{g'} \in G/H$ if and only if $g = g'h$ for some $h \in H$. So for every $h \in H$, we have $\underline{h} = \underline{e}$.

So the idea of G/H is that G/H is the most "efficient" group one can make while demanding that $h = e$ for all $h \in H$. But what if you some arbitrary collection elements that you want to make trivial? In general, given any subset $A \subseteq G$, we can ask for the most efficient group obtained by forcing all $a \in A$ to equal e_G.

Example 10.4. Take $G = S_n$ and $A = \{(12)\}$. How would you make (12) into e? You might be tempted to just take $G/\langle A\rangle$, but we don't know if $\langle A\rangle$ is normal. So instead, we let N_A denote the smallest *normal* subgroup of G containing A, and then take G/N_A.

Proposition 10.5. *Let $A, N_A \subseteq G$ be subsets. The following are equivalent:*

(1) N_A is the smallest non-empty subset of G containing A and closed under multiplication, inverses, and conjugates by elements of G.

(2) N_A is the set of all elements in G that can be written as a product

$$\cdots g a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} g^{-1} h b_1^{m_1} \cdots b_l^{m_l} h^{-1} \cdots$$

(this is really impossible to write down) where $a_i, b_i, g, h, \ldots \in A$ and $n_i, m_i, \ldots \in \mathbb{Z}$.

(3) N_A is the smallest normal subgroup containing A.

(4) Let J be the set of all normal subgroups of G that contain A. Then $N_A = \bigcap_{H \in J} H$.

So what happens in our example? Because N_A is normal, conjugates of (12) should also be in N_A. This means that all swaps (ij) are in N_A. But the transpositions generate the entire group S_n, so $N_A = G$. That is, crushing (12) to the identity results in everything getting crushed to the identity.

Example 10.6. Let $A = \{xyx^{-1}y^{-1}\}_{x,y \in G}$. In this dream world where A becomes the identity, everything commutes, i.e., the group becomes abelian. But note that $[G, G]$ is the group generated by A and $[G, G]$ is normal. So $N_A = [G, G]$ and

$$G/[G, G]$$

is the abelianization that makes G into abelian in the most efficient way.

There is also a notion of how much G was already abelian.

Definition 10.7. The **center** $Z(G)$ is

$$Z(G) = \{x : xg = gx \text{ for all } g \in G\}.$$

This is nonempty, because it contains the identity. It is also a subgroup.

11 September 29, 2017

Recall that a group isomorphism is a bijection $\phi : G \to H$ such that ϕ is a group homomorphism.

Exercise 11.1. If $\phi_1 : G \to H$ and $\phi_2 : H \to I$ are group isomorphisms, then $\phi_2 \circ \phi_1$ is a group isomorphism and ϕ^{-1} are group isomorphisms.

We write $G \cong H$ when G admits a group isomorphism to H. In this case, we say that "G is isomorphic to H".

On the other hand, suppose $\phi : G \to H$ is a group isomorphism. Then $g \in G$ and $\phi(g) \in H$ "play the same roles" in their respective groups. That is, group isomorphisms preserve any meaningful property of a group or an element of a group can have. For example, G and H have the same number of elements of order 13.

There exist group isomorphisms G to itself. We already know that G is the same as G. That is, $\mathrm{id}_G : G \to G$ is a group isomorphism. But there are other interesting group isomorphisms.

Example 11.2. Consider the mattress group $G = \{e, R_x, R_y, R_z\}$. But there is no reason that R_x, R_y, or R_z to be privileged to other. So there exist group isomorphisms of G to itself taking $\{R_x, R_y, R_z\}$ to $\{R_x, R_y, R_z\}$ in any way.

11.1 Conjugation

Definition 11.3. Let X be a set. We define

$$\mathrm{Aut}_{\mathsf{Set}}(X) = \{\text{bijections } X \to X\}.$$

Let G be a group. Similarly, we define

$$\mathrm{Aut}(G) = \{\text{group isomorphisms from } G \text{ to itself}\}.$$

A group isomorphism $G \to G$ is called a **group automorphism**.

Exercise 11.4. $\mathrm{Aut}(G)$ is a group under composition.

Solution. The identity id_G is the identity $e_{\mathrm{Aut}(G)}$, ϕ^{-1} is the inverse, and $\mathrm{Aut}(G)$ is closed under composition. □

Definition 11.5. Fix $g \in G$ and $x \in G$. Then the **conjugation** of x by g is the element $gxg^{-1}G$. This defines a function

$$\Phi_g : G \to G; \quad x \mapsto gxg^{-1}.$$

Note that Φ_g is a bijection, because

$$\Phi_{g^{-1}} \circ \Phi_g(x) = g^{-1}(gxg^{-1})g = x$$

and likewise $\Phi_g \circ \Phi_{g^{-1}} = \mathrm{id}_G$. Also, Φ_g is a group homomorphism. This is because

$$\Phi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \Phi_g(x)\Phi_g(y).$$

That is, for every $g \in G$, we have a group automorphism Φ_g of G.

Now we have a function

$$\Phi : G \to \mathrm{Aut}(G); \quad g \mapsto \Phi_g.$$

Is it a group homomorphism? We can check

$$\Phi_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \Phi_g(\Phi_h(x)).$$

Exercise 11.6. Compute $\ker(\Phi)$.

Solution. The kernel is the center $Z(G) = \{g : gx = xg \text{ for all } x \in G\}$. This is because

$$\begin{aligned}\ker(\Phi) &= \{g : \Phi_g = \mathrm{id}_G\} = \{g : gxg^{-1} = x \text{ for all } x \in G\} \\ &= \{g : gx = xg \text{ for all } x \in G\} = Z(G).\end{aligned}$$

□

11.2 Conjugacy class

If conjugate elements play the same role in a group, why don't we try to determine all the elements in a group that are conjugate?

Definition 11.7. The **conjugacy class** of an element $x \in G$ is the set of all y such that $gyg^{-1} = x$ for some $g \in G$.

Observe that there is a map

$$G \to \mathrm{Aut}(G) \hookrightarrow \mathrm{Aut}_{\mathsf{Set}}(G),$$

that is, conjugation is an action of G on the set G. Explicitly, this is given by

$$\mu : G \times G \to G; \quad (g, x) \mapsto gxg^{-1}.$$

So the conjugacy class of $x \in G$ is just the orbit of x under this action.

We can count using this! Note that

$$G = \bigcup_{\text{orbits } I} I = \bigcup_{\text{conj. class } I} I.$$

Since conjugacy classes are disjoint, we get

$$|G| = \sum_{\text{conj. class } I} |I|.$$

But we know that for any group action $H \times X \to X$, we know how to compute the size of the orbit. It is $|\mathcal{O}_x| = |H|/|H_x|$, where $H_x = \{h \in H : hx = x\}$.

Exercise 11.8. Find all $x \in G$ such that the size of its conjugacy class is $|\mathcal{O}_x| = 1$.

Solution. We claim that $|\mathcal{O}_x| = 1$ if and only if $x \in Z(G)$. This is because they are both equivalent to $gxg^{-1} = x$ for all $g \in G$. □

11.3 Classifying groups of prime power order I

Now you are about to become very powerful.

Theorem 11.9. *Let G be a finite group such that $|G| = p^N$ for some prime p. Then $Z(G)$ is nontrivial.*

Example 11.10. The quaternions Q_8 has size $8 = 2^3$, and ± 1 is the center. The dihedral group D_8 also has size 2^3, and r^2 commutes with everything.

Theorem 11.11. *Any group of order p^2 is abelian, and isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Now let's prove them.

Proof of Theorem 11.9. By the class equation,

$$|G| = \sum |I| = 1 + \cdots + 1 + \sum_{|I| \geq 2} |I| = |Z(G)| + \sum_{|I| \geq 2} |I|,$$

because orbits of size 1 are elements in the center. But note that $|I|$ divides $|G| = p^N$. So if $|I| \geq 2$, it is a prime power of p with exponent at least 1. So we have

$$p^N = |Z(G)| + p(\cdots)$$

and so p divides $|Z(G)|$. But $|Z(G)| > 0$ and so there are at least p elements in $Z(G)$. □

Proof of Theorem 11.11. It's basically the same thing. We know that either $|Z(G)| = p$ or $|Z(G)| = p^2$. But if there exists an element of $x \in Z(G)$, then the stabilizer G_x contains $Z(G) \cup \{x\}$, which has size greater than p. But G_x is a subgroup of G and so has order power of p. So $G_x = G$ and we get a contradiction. This means that $Z(G) = G$ and G is abelian. □

12 October 2, 2017

Last time we defined a conjugation action $G \times G \to G$ given by $(g, x) \mapsto gxg^{-1}$. Then we talked about counting, or the class equation

$$|G| = \sum_{I \text{ conjugacy class}} |eI|.$$

12.1 Classifying groups of prime power order II

Definition 12.1. Fix $x \in G$. The stabilizer (of x) for the conjugation action is called the **centralizer** of x,

$$C_G(x) = \{g \in G : gx = xg\}.$$

I stated two theorems.

Theorem 12.2. *If $|G| = p^N$ with p prime and $N > 1$, then $|Z(G)| \geq p$.*

Theorem 12.3. *If $|G| = p^2$, then G is abelian and is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proof. To show that G is abelian, we need to show that $|Z(G)| = p^2$. We know from the previous theorem, that either $|Z(G)| = p$ or $|Z(G)| = p^2$. Assuming $|Z(G)| = p$, choose $x \in G$ such that $x \notin Z(G)$. Then the conjugacy class I of x satisfies

$$|I| = |G|/|C_G(x)|.$$

But $C_G(x)$ contains $Z(G)$ and x. So $|C_G(x)| \geq p + 1$ but C_G is a subgroup of G. This shows that $|C_G(x)| = p^2$ and $C_G(x) = G$. This contradicts our assumptions that $x \notin Z(G)$. That is, $Z(G) = G$ and G is abelian.

Now assume that $G \ncong \mathbb{Z}/p^2\mathbb{Z}$. Then every element $x \neq e$ has order p, because it can't have order p^2. Now fix $x \in G$ such that $x \neq e$. Then $\langle x \rangle \subseteq G$ has order p. So choose $y \notin \langle x \rangle$. We claim is that $\langle x \rangle \cap \langle y \rangle = \{e\}$. Assuming this fact, we can define

$$\phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G; \quad (a, b) \mapsto x^a y^b.$$

This is well-defined because x, y have order p, and is a homomorphism because G is abelian and so $(x^a y^b)(x^{a'} y^{b'}) = x^{a+a'} y^{b+b'}$. What is the kernel? If $x^a y^b = e$, then $x^a = y^{-b}$ and so $x^a, y^b \in \langle x \rangle \cap \langle y \rangle = \{e\}$. This means that $x^a = y^b = e$ and so $a, b = 0 \pmod{p}$. Then ϕ has trivial kernel and hence an injection. But both sides have p^2 elements and because it is an injection, it has to be a bijection. That is, ϕ is a group isomorphism.

Now we have to show the claim that $\langle x \rangle \cap \langle y \rangle = \{e\}$. Assume that $x^a = y^b$ for some $0 < a, b < p$. Then $\gcd(b, p) = 1$ and so there are integers $b \in \mathbb{Z}$ such that $Ap + Bb = 1$. Then

$$\langle x \rangle \ni (x^a)^B = (y^b)^B = y^{1-Ap} = y.$$

This contradicts $y \notin \langle x \rangle$. □

12.2 The fundamental group

Definition 12.4 (for today)**.** A **space** is a subset $X \subseteq \mathbb{R}^n$.

For example, we have spaces $X = \mathbb{R}^2 \setminus \{0\}$ and $X = S^1$. To each X, we are going to associate a group $\pi_1(X)$. It's sometimes not easy to visualize spaces, and group will be useful to analyze these spaces. For instance, π_1 is an invariant, i.e., if $\pi_1(X) \ncong \pi_2(Y)$, then $X \ncong Y$.

Definition 12.5. Fix a space X. A **path** in X is the data of (γ, T), where $T \geq 0$ and $\gamma : [0, T] \to X$ is continuous. We say that γ is a **loop** is closed if $\gamma(0) = \gamma(T)$.

Fix some point $x \in X$, and call it the base point.

Definition 12.6. The **Moore path space** of X at x is the set of all closed paths (γ, T) such that $\gamma(0) = \gamma(T) = x$.

The claim is that this is becoming to look like a group. How do you compose two paths (γ, T) and (γ', T')? As soon as we finish the first loop, we can start the second loop. Define

$$\gamma * \gamma' : [0, T + T'] \to X; \quad t \mapsto \begin{cases} \gamma(t) & 0 \leq t \leq T \\ \gamma'(t - T) & T \leq t \leq T + T'. \end{cases}$$

There is also the identity

$$\gamma_e : [0, 0] \to X; \quad 0 \mapsto x.$$

But there is no inverse, because time only gets longer as we compose. So we need to modify it to have inverses.[5] We are going to declare $\gamma = \gamma'$ is γ can be obtained from γ' by "wiggling" and "reparetrizing". The **fundamental group** $\pi_1(X)$ is the group

$$\{(\gamma, T)\}/(\text{wiggle and reparametrization}).$$

The π_1 of the stage, which looks like a cube, is trivial. This is because you could always wiggle around the loop to near the basepoint.

What is the π_1 of the stage, but with a tall person standing on it. There is a nontrivial element, which is to go around between this person's legs. There is an inverse element, which is to go around in the opposite direction. It turns out that $\pi_1 \cong \mathbb{Z}$, because the element is determined by how many times the rope goes around the legs.

[5] This is going to be very handwavy. Look up homotopy if you want a precise definition.

13 October 4, 2017

Last time, for a space $X \subseteq \mathbb{R}^N$, we defined the fundamental group

$$\pi_1(X, x) = \pi_1(X) = \{(\gamma, T) : (\gamma : [0, T] \to X) \text{ with } \gamma(0) = \gamma(1) = x\}/\sim$$

where $\sim$ is wiggling and reparametrization. If X is the stage with James, we saw that $\pi_1(X) \cong \mathbb{Z}$.

Let X and Y be two space, and consider $f : X \to Y$ be a continuous function. Then from a path in X, I get a path in Y. That is, we have a function

$$\{(\gamma, T) : [0, T] \to X\} \to \{(\gamma', T') : [0, T'] \to Y\}; \quad (\gamma, T) \mapsto (f \circ \gamma, T).$$

This assignment respect the equivalences. This is because if I wiggle something in X and compose with f, it is going to be a wiggle in Y. It also respects composition.

Proposition 13.1. *Every continuous $f : X \to Y$ induces a group homomorphism $\pi_1(X) \to \pi_1(Y)$.*

This is actually a powerful fact. If you manage to wiggle X into Y and Y into X, then you conclude that $\pi_1(X)$ and $\pi_1(Y)$ are isomorphic. Here is another cool fact.

Theorem 13.2. *Assume $\pi_1 X = *$, like $X = \mathbb{R}^3$ or $X = \mathbb{R}^2$ or $X = S^2$. Assume we have a group action $G \times X \to X$ such that*

(1) for all $g \in G$, the map $X \to X$; $x \mapsto gx$ is continuous,

(2) for every $x \in X$, there is a small open ball U containing x such that $gU \cap hU = \emptyset$ if $g \neq h$.

Then the orbits X/G is a space and $\pi_1(X/G) \cong G$.

Example 13.3. Let $X = \mathbb{R}$ and $G = \mathbb{Z}$. The integers act on $\mathbb{R}$ by translations. Then the theorem states that

$$\pi_1(S^1) = \pi_1(\mathbb{R}/\mathbb{Z}) \cong \mathbb{Z}.$$

Example 13.4. In an optional problem, you might have shown that there is a group homomorphism

$$S^3 \cong \mathrm{SU}(2) \xrightarrow{\pi} \mathrm{SO}(3),$$

with kernel $\mathbb{Z}/2\mathbb{Z}$. Because $\pi_1(S^3) = *$, what this shows is that $\pi_1(\mathrm{SO}(3)) \cong \mathbb{Z}/2\mathbb{Z}$.

13.1 Elliptic curves

Definition 13.5. An **elliptic curve** is the set of solutions $\{(x, y)\}$ to an equation of the form

$$y^2 = x^3 + ax + b$$

for $a, b \in \mathbb{R}$, such that every point on my curve has a well-defined tangent line.

Let's try to visualize this curve. There are many possibilities, but if the equation $x^3 + ax + b$ have distinct three real roots, it is going to look like Figure 3.

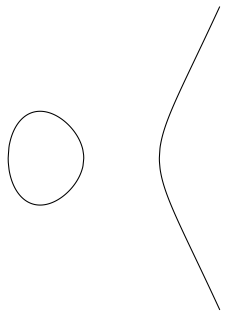


Figure 3: Solution to $y^2 = x^3 - x$

Proposition 13.6. *Let $E = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\infty\}$. Then E admits the structure of an abelian group.*

Exercise 13.7. Fix two points (x_1, y_1) and (x_2, y_2) solving the equation. Assume that the line L containing them is not vertical. Show that L intersect another point on the curve.

Solution. In general, fix a (non-vertical line)

$$L = \{(x, y) : mx + y_0 = y\}.$$

Then $(x, y) \in L \cap E$ is equivalent to

$$(mx + y_0)^2 = x^3 + ax + b.$$

This is a cubic equation in x, and we know two roots. So there exists a third root x_3 and then we could get $y_3 = mx_3 + y_0$. □

Definition 13.8. Set the addition $E \times E \to E$; $(P, Q) \mapsto P + Q$ to be

(1) If the line through P and Q is not vertical, let R be the "third intersection point" of the line and E. Then we set $P + Q = \overline{R}$, the reflection of R about the x-axis.
(2) If P and Q lie on a vertical line, then we let $P + Q = \infty$.
(3) If P or Q is ∞, then $P + \infty = P$ and $Q + \infty = Q$.

You can think of ∞ as a point that is infinitely far away in the vertical direction. So if you add ∞, you use a vertical line passing through P, look at the intersection, and then reflect. Then $P + \infty = P$.

Proposition 13.9. *The above makes E into an abelian group.*

Proof. The element ∞ is the unit. Also, given $P = (x, y)$, the $\overline{P} = (x, -y)$ is the inverse. Associativity is really hard, but you can try to visually see this by drawing it. □

14 October 6, 2017

Last time we defined an elliptic curve as

$$E = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\infty\},$$

and also

$$E(\mathbb{Q}) = \{(x, y) \in E : x, y \in \mathbb{Q}\} \subseteq E.$$

There was also a group structure on it that was, take the line through P and Q and flit the third intersection point about the x axis.

Exercise 14.1. (1) Show that E is abelian.

(2) Show that $(P, Q) \mapsto P + Q$ is associative. (Work out an example on the sheet.)

(3) Show that $E(\mathbb{Q})$ is a subgroup of $a, b \in \mathbb{Q}$.

How would you go about to prove associativity? You could use brute force. Another way is to prove this is to find an isomorphism with some other group and conclude that it is associative. This other group is going to be the space of line bundles with tensor product.

Solution. (a) The line through P and Q is the line through Q and P.

(b) You can draw some examples.

(c) Pick $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ in $\mathbb{Q}^2$. Then the line $y = mx + y_0$ has rational coefficients and so

$$x^3 + ax + b - (mx + y_0)^2 = x^3 + Ax^2 + Bx + C = (x - x_1)(x - x_2)(x - x_3).$$

So because $A = -m^2$ is rational and x_1, x_2 are rational, we get that x_3 is rational. Then $y_3 = mx_3 + y_0$ is rational. □

We can now ask some fundamental question about these groups. Can E be finitely generated? The answer is no, because a finitely generated group has to be countable but E has a continuum number of points. But is $E(\mathbb{Q})$ finitely generated? This is a hard question, and led to developments in number theory.

Theorem 14.2 (Mordell–Weil)**.** *Let $a, b \in \mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.*

We will see this later, but a finitely generated abelian group is isomorphic to some $\mathbb{Z}^N \times$ (finite abelian).

14.1 Finite subgroups of SO(3)

Today, I will find all finite subgroups of SO(3).

Definition 14.3. The **orthogonal group** O(3) is defined as

$$\mathrm{O}(3) = \mathrm{O}_3(\mathbb{R}) = \{3 \times 3 \text{ matrices } A \text{ with } \mathbb{R} \text{ entries such that } A^T A = I\}.$$

Then $A \in \mathrm{O}(3)$ is equivalent to $\langle u, v\rangle = \langle Au, Av\rangle$ for all $u, v \in \mathbb{R}$. In this case, $1 = \det(A)\det(A^T) = \det(A)^2$, so $\det(A) = \pm 1$.

Definition 14.4. We define the **special orthogonal group** $\mathrm{SO}(3)$ as

$$\mathrm{SO}(3) = \mathrm{SO}_3(\mathbb{R}) = \{A \text{ such that } A^T A = I \text{ and } \det(A) = 1\}.$$

Example 14.5. The identity matrix is in $\mathrm{SO}(3)$. Other matrices like

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & -\cos\theta \end{pmatrix}$$

are also in $\mathrm{SO}(3)$.

Theorem 14.6 (Euler's rotation theorem)**.** *Any $A \in \mathrm{SO}(3)$ is a rotation about some line through the origin.*

So any composition of two rotations is again a rotation. This a non-obvious feature of three-dimensional geometry. Let's prove this theorem.

Proof. We will prove that each $A \in \mathrm{SO}(3)$ has a $+1$ as an eigenvalue. If this is true, there exists a $v_1 \neq 0$ such that $Av_1 = v_1$. Using Gram–Schmidt, we can complete v_1 to an orthonormal basis v_1, v_2, v_3 and consider the matrix

$$B = \begin{pmatrix} v_1 & v_2 & v_3 \\ & & \end{pmatrix}.$$

Then we have $B^{-1}ABe_1 = B^{-1}Av_1 = B^{-1}v_1 = e_1$. So we can write

$$B^{-1}AB = \begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

But we have $\det(B^{-1}AB) = \det(A) = 1$ and

$$(B^{-1}AB)^T(B^{-1}AB) = B^T A^T B B^{-1} AB = 1.$$

So $B^{-1}AB \in \mathrm{SO}(3)$. This shows that the matrix has to take the form

$$B^{-1}AB = \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

Now it is an easy exercise to show that 2×2 region need to be a rotation. □

Theorem 14.7. *Any finite subgroup of* $\mathrm{SO}(3)$ *is isomorphic to one of the following:*

- $\mathbb{Z}/n\mathbb{Z}$ *for* $n > 0$

- D_{2n} *for* $n \geq 2$
- *symmetries of the tetrahedron* $\cong A_4$
- *symmetries of the cube* $\cong$ *symmetries of the octahedron* $\cong S_4$
- *symmetries of the dodecahedron* $\cong$ *symmetries of icosahedron* $\cong A_5$

Here, symmetries of cubes are the symmetries of the octahedron, because you can look at the centers of faces in a cube and it is a octahedron. Likewise, the centers of faces in a dodecahedron form a icosahedron.

15 October 11, 2017

Today I am going to give an idea of how to classify all finite subgroups of $\mathrm{SO}_3(\mathbb{R})$. Here, recall that $\mathrm{SO}_3(\mathbb{R})$ is the group of all 3×3 matrices with $\mathbb{R}$-entries, sch that $A^T A = I$ and $\det A = 1$.

Lemma 15.1. *Any $A \in \mathrm{SO}_3$ has $+1$ as an eigenvalue.*

Proof. It suffices to show $\det(A - I) = 0$. This would imply that there exists a $v \neq 0$ such that $Av = Iv = v$. We have

$$\begin{aligned}\det(A - I) &= \det(A)\det(A - I) = \det(A^T)\det(A - I) = \det(A^T A - A^T) \\ &= \det(I - A^T) = \det(I - A) = (-1)^3 \det(A - I).\end{aligned}$$

This shows that $\det(A - I) = 0$. □

Corollary 15.2. *Any $A \in \mathrm{SO}_3$ is a rotation of some angle about some axis.*

15.1 Classifying finite subgroups of SO_3 I

Theorem 15.3. *Let $G \subseteq \mathrm{SO}_3$ be a finite subgroup. Then G is isomorphic to one of the following:*

(1) $\mathbb{Z}/n\mathbb{Z}$

(2) D_{2n}, which is the symmetry of a prism with face of a regular n-gon

(3) symmetries of the tetrahedron (or A_4)

(4) symmetries of a cube/octahedron (or S_4)

(5) symmetries of a dodecahedron/icosahedron (or A_5)

Definition 15.4. Recall that there is a group homomorhism

$$\mathrm{sign} : S_n \to \mathbb{Z}/2\mathbb{Z}.$$

We define the **alternating group** as $A_n = \ker(\mathrm{sign})$.

Why are the symmetry groups of shapes isomorphic to the symmetry groups of sets? Let's look at (3) for instance. Any symmetry $A \in \mathrm{SO}_3$ sends the four vertices of the tetrahedron to the same four vertices, so there is a map

$$\mathrm{Symm}(\text{tetrahedron}) \to S_4,$$

which is injective. Then we only need to identify those vertex permutations that actually come from a rotation. Because $\mathbb{R}^3$ has an orientation, such an element should be in A_4. Conversely, any element in A_4 comes from a rotation.

What about for cubes? There is a map

$$\mathrm{Symm}(\text{cube}) \to S_4,$$

by sending diagonals to diagonals. You can then verify that this is an isomorphism. For dodecahedrons, it turns out there are five cubes that can be circumscribed inside a well-drawn dodecahedron. The isomorphism comes from this action.

Definition 15.5. For a nontrivial finite subgroup $G \subseteq \mathrm{SO}(3)$, define

$$P = \{v \in \mathbb{R}^3 : \|v\| = 1,\ gv = v \text{ for some } g \neq e\}.$$

This set is nonempty, by the lemma that every rotation has $+1$ has an eigenvector. There exists a $v \neq 0$ such that $Av = v$, and then $v/\|v\|$ and $-v/\|v\|$ are in P. Moreover, if $g \neq e$, there are exactly two points in P, so we see that P is finite, having a most $2(|G| - 1)$ elements.

Exercise 15.6. For any $v \in P$ and $g \in G$, $gv \in P$.

Solution. We need to show that there exists $e \neq h' \in G$ such that $h'(gv) = gv$. Since $v \in P$, there exists an $h \neq e$ such that $hv = v$. So let $h' = ghg^{-1}$. Then

$$h'(gv) = (ghg^{-1})(gv) = g(hv) = gv.$$

Also, $h' \neq e$. □

The point is that there is a group action of G on P. Now we are going to count elements in two different ways.

Lemma 15.7 (Main lemma)**.** *This group action has at most three orbits.*

Proof. Define

$$A = \{(g, v) : g \neq e,\ gv = v\} \subseteq G \times V.$$

For each $e \neq g \in G$, there are exactly two v that is fixed under G. This shows $\#A = 2(|G| - 1)$. On the other hand, for a fixed v, there are $|\mathrm{Stab}(v)| - 1$ such $g \neq e$ fixing g. So

$$\#A = 2(|G| - 1) = \sum_{v \in P} (|\mathrm{Stab}(v)| - 1).$$

But recall that if u and v are in the same orbit, then $|\mathrm{Stab}(u)| = |\mathrm{Stab}(v)|$. Let us regroup the sum by orbits. Then

$$2(|G| - 1) = \sum_{\text{orbits } \mathcal{O}} |\mathcal{O}| \Big(\frac{|G|}{|\mathcal{O}|} - 1 \Big).$$

Let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be the orbits and write $s - i = |\mathrm{Stab}(v_i)|$ with $v_i \in \mathcal{O}_i$. After dividing both sides by $|G|$, we get

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r} \Big(1 - \frac{1}{s_i} \Big),$$

The claim is that this just implies $r \leq 3$. This is because $s_i \geq 2$ by the definition of P, and then each term on the right hand side is at least $1/2$. □

Now we have either 1, 2, or 3 orbits, and the corresponding s_i. So we must find the possible values of s_i such that

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r} \Big(1 - \frac{1}{s_i}\Big)$$

can hold.

Clearly $r = 1$ cannot hold, because the right hand side is less than 1 and the left hand side is at least 1. The other cases are:

- $(s_1, s_2) = (n, n)$, which is when $G \cong \mathbb{Z}/n\mathbb{Z}$,
- $(s_1, s_2, s_3) = (2, 2, n)$, which is when $G \cong D_{2n}$,
- $(s_1, s_2, s_3) = (2, 2, 3)$, which is when G is the symmetries of the tetrahedron,
- $(s_1, s_2, s_3) = (2, 3, 4)$, which is when G is the symmetries of the cube,
- $(s_1, s_2, s_3) = (2, 3, 5)$, which is when G is the symmetries of the dodecahedron.

16 October 13, 2017

16.1 Classifying finite subgroups of SO_3 II

Last time we classified finite subgroups $G \subseteq \mathrm{SO}_3$. We defined

$$P = \{v \in \mathbb{R}^3 : \|v\| = 1,\ gv = v \text{ for some } g \neq e\}.$$

By counting $\{(g, v) : gv = v\}$, we arrived at the formula

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r} \Big(1 - \frac{1}{s_i}\Big),$$

where r is the number of orbits and s_i is order of the stabilizer of $v \in \mathcal{O}_i$.

Corollary 16.1. *There are at most 3 orbits in the G-action of P.*

Proof. Note that $1 \leq 2 - \frac{2}{|G|} < 2$ if $|G| \geq 2$. On the other hand, if $s_i \geq 2$ then $1 - \frac{1}{s_i} \geq \frac{1}{2}$. Then

$$\frac{1}{2}r \leq \Big(1 - \frac{1}{s_1}\Big) + \cdots + \Big(1 - \frac{1}{s_r}\Big) < 2.$$

So $r \leq 3$. □

There is no college math going on. We're only using facts about how big or small numbers can be.

Corollary 16.2. *There exist at least two orbits.*

Proof. $2 - \frac{2}{|G|} \geq 1$, while $1 - \frac{1}{s_1} < 1$. □

So now let's play around with these numbers. What are the possible combinations of (s_1, s_2)? Without loss of generality, assume $s_1 \leq s_2$. We are solving $2 - \frac{2}{|G|} = 2 - \frac{1}{s_1} - \frac{1}{s_2}$, and so

$$\frac{\|G\|}{s_1} + \frac{|G|}{s_2} = 2.$$

But both terms are positive integers, and so we get $|G| = s_1 = s_2$. If $v \in P$, then all elements of G fix v, and G should be the rotations. Then $G \cong \mathbb{Z}/n\mathbb{Z}$ is the rotational symmetries of the regular n-gon.

Now let's look at the case $r = 3$. We still have the formula

$$2 - \frac{2}{|G|} = 3 - \frac{1}{s_1} - \frac{1}{s_2} - \frac{1}{s_3}.$$

We can assume without loss of generality that $s_1 \leq s_2 \leq s_3$.

Exercise 16.3. $s_1 \leq 2$.

Solution. If $3 \leq s_1 \leq s_2 \leq s_3$, then

$$1 \leq \frac{1}{s_1} + \frac{1}{s_2} + \frac{1}{s_3} = 1 + \frac{2}{|G|}. \qquad \square$$

If you more inequalities, you see that the only possibilities are

$$(s_1, s_2, s_3) \in \{(2,2,2), (2,2,3), (2,2,4), \ldots, (2,3,3), (2,3,4), (2,3,5)\}.$$

If $(s_1, s_2, s_3) = (2, 2, n)$, then $|G| = 2n$ by the formula. Let $v \in P$ be the point in the orbit with stabilizer of size n. Then this stabilizer $\mathrm{Stab}(v)$ is going to be the rotational group $\mathbb{Z}/n\mathbb{Z}$. Because the stabilizer of v has size n, the orbit has size 2. But this rotation group also fixes the antipode of v, and so (assuming that $n \geq 3$) the orbit of v is $\{v, -v\}$. Then it can be checked that the group G has to be the dihedral group.

For (s_1, s_2, s_3) equals $(2,3,3)$, $(2,3,4)$, $(2,3,5)$, check this when you go back home.

16.2 Equivalence classes

You have seen this in high school. When dealing with angles, we always say $360 = 0$ or $2\pi = 0 = 4\pi$. But this is not actually true. The point of equivalence classes is to produce new set where these equations are literally true.

Definition 16.4 (Definition A)**.** Fix a set $X \neq \emptyset$. An **equivalence relation** R is a subset of $X \times X$, satisfying

(1) The diagonal is contained in R, i.e., $(x, x) \in R$ for all $x \in X$.

(2) If $(x, y) \in R$ and $(y, x) \in R$, then $(x, z) \in R$.

(3) If $(x, y) \in R$ then $(y, x) \in R$.

We are going to use the notation $x \sim y$ if and only if $(x, y) \in R$. So for instance $x \sim y$ and $y \sim z$ implies $x \sim z$.

Definition 16.5 (Definition B)**.** A **partition** of X is a collection $\mathcal{I}$ of subsets of X such that

(1) $\bigcup_{I \in \mathcal{I}} I = X$.

(2) $I \neq \emptyset$ for all $I \in \mathcal{I}$.

(3) For all $I, J \in \mathcal{I}$, if $I \cap J \neq \emptyset$ then $I = J$.

Definition 16.6 (Definition C)**.** A **surjection** out of X is a function

$$X \to D$$

which is a surjection.

Definition 16.7 (Definition D)**.** A **partition** of X is a function

$$\pi : X \to \mathcal{P}(X) = \{I : I \subseteq X\}$$

such that $\pi^{-1}(I) = I$ when $\pi^{-1}(I) \neq \emptyset$.

These are actually all the same thing. In Definition C, the set D is the place where you can write $0 = 360$. Let's denote this function $X \to D$ as $x \mapsto [x]$. Then even if $x \neq y$, we can have $[x] = [y]$.

Proof of (A) $\Rightarrow$ (B). Given R, call a subset $I \subseteq X$ an **equivalence class** (for R) if

- $I \neq \emptyset$,
- for all $x \in I$, $y \sim x$ implies $y \in I$,
- if $x, y \in I$ then $x \sim y$.

Now let $\mathcal{I}$ be the set of equivalence classes. Then $\mathcal{I}$ is a partition of X, because if $x \in I \cap J$, then I and J are both just the set of y such that $x \sim y$. □

Proof of (B) $\Rightarrow$ (D). Given a partition $\mathcal{I}$ of X, consider the function

$$X \to \mathcal{P}(X); \quad x \mapsto I = \{y \in X : y \sim x\}.$$

This satisfies $\pi^{-1}(I) = I$ for $\pi^{-1}(I) \neq \emptyset$. You can verify this from the definition. □

Proof of (D) $\Rightarrow$ (C). Just set $D = \text{image}(\pi)$. □

Proof of (C) $\Rightarrow$ (A). Given a surjection $p : X \to D$, define R by $(x, y) \in R$ if and only if $p(x) = p(y)$. □

Definition 16.8. Given an equivalence relation R and $x \in X$, we say that the unique $I \in \mathcal{I}$ such that $x \in I$ is the **equivalence class** of X.

17 October 16, 2017

What can we do with integers? We can add them, of course. $\mathbb{Z}$ is a group with addition, so there is an additive identity $0 \in \mathbb{Z}$, and there is addition and subtraction. But there is multiplication, primeness, factorization, quotients.

17.1 Rings

Definition 17.1. A **ring** is the data of

- a set R
- a function $+ : R \times R \to R$; $(a, b) \mapsto a + b$
- a function $\times : R \times R \to R$; $(a, b) \mapsto ab$

satisfying

(1) $(R, +)$ is an abelian group, (i.e., there exists a $0 \in R$ such that $0 + a = a + 0 = a$ for all a, and for all $a \in R$ there exists an additive $-a \in R$ such that $a + (-a) = 0$)

(2a) $\times$ has a unit (i.e., there exists a $1 \in R$ such that $1a = a1 = a$ for all $a \in R$)

(2b) $\times$ is associative (i.e., $a(bc) = (ab)c$ for all $a, b, c \in R$)

(3) distributivity (i.e., $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$).

Example 17.2. Here are some examples.

- $R = \mathbb{Z}$ is a ring with usual addition and multiplication.
- $R = \mathbb{Z}/n\mathbb{Z}$ is a ring with usual addition and multiplication. They are given by $a + b = (a + b) \bmod n$ and $ab = (ab) \bmod n$.
- $R = \mathcal{M}_{n\times n}(\mathbb{R})$, the $n \times n$ matrices with real entries, is a ring with addition and matrix multiplication.
- If R is a ring in general, then $\mathcal{M}_{n\times n}(R)$ with entries in R is also a ring.
- Fix A and abelian group, and let $R = \mathrm{Hom}(A, A)$ be the set of all homomorphisms from A to A. There is pointwise addition and composition. Under these operations, R is a ring.
- For R a ring, the polynomials in x with coefficients in R, denoted by $R[x]$, is a ring with normal addition and multiplication. The set of power series, denoted by $R[[x]]$, is also a ring.

Exercise 17.3. Show that for A an abelian group, $R = \mathrm{Hom}(A, A)$ is a ring.

Solution. Let's first show that R is an abelian group under addition. The unit is the $0 : A \to A$ with $a \mapsto 0$ for all $a \in A$. Now

$$(f + (g + h))(a) = f(a) + (g + h)(a) = f(a) + g(a) + h(a) = ((f + g) + h)(a)$$

and the inverse is $-f : a \mapsto -f(a)$. The function $-f$ is still a group homomorphism because

$$-f(a+b) = -(f(a+b)) = -(f(a)+f(b)) = (-f(a)) + (-f(b)).$$

Also, $f + g = g + f$ can be checked because A is abelian.

Now we need to show that that multiplication has a unit and is associative. The unit is the identity map $\mathrm{id}_A : A \to A$, because composition by identity doesn't do anything. Associativity follows from associativity of composition.

We now check distributivity. We have

$$(f(g+h))(a) = f(g(a)+h(a)) = fg(a) + fh(a) = (fg+fh)(a)$$

and right distributivity follows likewise. □

Definition 17.4. For A an abelian group, then

$$\mathrm{End}(A) = \mathrm{Hom}(A, A)$$

is called the **ring of endomorphisms**.

17.2 Useful properties of rings

There are certain things you are used to in $\mathbb{Z}$ that aren't contained in the definition of a ring. You will be able to show this.

Exercise 17.5. Let R be a ring. Prove the following:

(i) For all $a \in R$, $0 \cdot a = a \cdot 0 = 0$.

(ii) For all $a \in R$, $(-1) \cdot a = -a = a \cdot (-1)$

(iii) Assume there exist u, v such that $ux = 1$ and $xv = 1$. Show that $u = v$.

Solution. (i) We don't have that much to work with. We have

$$1 \cdot a = (0+1) \cdot a = 0 \cdot a + 1 \cdot a.$$

By the cancellation law, we get $0 = 0 \cdot a$.

(ii) Again, we have

$$0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a.$$

So $(-1) \cdot a = -a$.

(iii) We have

$$u = u \cdot 1 = u \cdot xv = ux \cdot v = 1 \cdot v = v.$$ □

Definition 17.6. A ring R is called **commutative** if $ab = ba$ for all $a, b \in R$.

Definition 17.7. Fix a ring R. An element $x \in R$ is called a **unit** if there exists an u such that $xu = ux = 1$.

Let $R^\times = \{x \in R : x \text{ is a unit}\}$. Then $R^\times$ is a group.

Example 17.8. If $R = \mathcal{M}_{2\times 2}(\mathbb{R})$ then $R^\times \mathrm{GL}_2(\mathbb{R})$.

Example 17.9. If $R = \mathrm{End}(A)$ for some abelian group A, then $R^\times = \mathrm{Aut}(A)$.

18 October 18, 2017

Last time we defined rings R and units $R^\times \subseteq R$, gave some examples, and proved basic properties.

Definition 18.1. Fix the data of a set R with functions $+, \times : R \times R \to R$ such that $(R, +)$ is an abelian group, $\times$ is associative and unital, and $\times$ distributes over $+$.

Examples include $\mathrm{End}(A)$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Definition 18.2. Given a commutative ring R, the **polynomial ring** $R[x]$ on one generator is the following ring:

- $R[x]$ is the set of polynomials with variable x and coefficients in R. Formally,
$$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n : a_i \in R \right\}.$$
- Addition is defined in the usual way as
$$\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{\max(m,n)} (a_k + b_k) x^k,$$
where we extend a_k or b_k to $k \leq \max(m, n)$ by 0.
- Multiplication is also defined as usual,
$$\left(\sum a_i x^i\right)\left(\sum b_j x^j\right) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x_k.$$

For example, we have $4 + 3x + 7x^2 \in \mathbb{Z}[x]$.

18.1 Ring homomorphism

Definition 18.3. Fix rings R and S rings. A function $\phi : R \to S$ is called a **ring homomorphism** if

- $\phi(x + y) = \phi(x) + \phi(y)$ and
- $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in R$, and also
- $\phi(1_R) = 1_S$.

The last axiom $\phi(1_R) = 1_S$ is something you realize in hindsight. With groups, we didn't need this definition because it followed from the $\phi(xy) = \phi(x)\phi(y)$. But the map $\mathbb{Z} \to \mathbb{Z}$ given by $x \mapsto 0$ satisfies the first two conditions but not the last. So this is not a ring homomorphism.

Definition 18.4. A ring homorphism is called a **ring isomorphism** if it is a bijection.

If $\phi : R \to S$ and $\psi : S \to T$ are ring homomorphisms, so is $\psi \circ \phi$. If ϕ is a ring isomoprhism, so is ϕ^{-1}.

Definition 18.5. Fix a ring R. Then a subset $S \subseteq R$ is called a **subring** if

- $-x, x+y, xy \in S$ for all $x, y \in S$,
- $0, 1 \in S$.

Exercise 18.6. Consider the function

$$\mathbb{C} \xrightarrow{\phi} \mathcal{M}_{2\times 2}(\mathbb{R}); \quad a+bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Show that ϕ is a ring homomorphism.

Solution. We can check $\phi(1) = I$ by $1 + 0i \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Also,

$$\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = \begin{pmatrix} a+c & -b-d \\ b+d & a+c \end{pmatrix}.$$

You can check multiplicaiton similarly. □

18.2 Kernel and image

Definition 18.7. Fix a ring homorphism $\phi : R \to S$. The **image** of ϕ is defined as

$$\phi(R) = \{s \in S : s = \phi(r) \text{ for some } r \in R\}.$$

The **kernel** is defined as

$$\ker(\phi) = \{r \in R : \phi(r) = 0\}.$$

Here, we have chosen kernel to be things that map to 0, not 1. This is going to help us in the long run.

Proposition 18.8. *The image* $\operatorname{im}(\phi) \subseteq S$ *is a subring.*

But the kernel is almost always never going to be a subring. This is because $\phi(1) = 1$ so $1 \notin \ker(\phi)$ if $1 \neq 0$. But it has a different structure.

Definition 18.9. A subset $I \subseteq R$ is called a **left ideal** if

(1) I is a subgroup of $(R, +)$,

(2l) I is closed under "scaling" from the left: $rx \in I$ for all $x \in I$ and $r \in R$.

Likewise, I is called a **right ideal** if

(1) I is a subgroup of $(R, +)$,

(2r) I is closed under "scaling" from the right: $xr \in I$ for all $x \in I$ and $r \in R$.

I is called a **two-sided ideal** if it is both a left ideal and a right ideal.

Exercise 18.10. For each ring homorphism $\phi : R \to S$, its kernel $\ker(\phi) \subseteq R$ is a two-sided ideal.

Solution. From what we know from groups, $\ker(\phi) \subseteq R$ is a subgroup. If $r \in R$ and $x \in I$, then

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0 = 0$$

shows that $rx \in \ker(\phi)$. For the other side, you can argue similarly. □

Theorem 18.11 (First isomorphism theorem)**.** *Fix $\phi : R \to S$. Then there exists a natural map*

$$R/\ker(\phi) \to \operatorname{im}(\phi)$$

and this is an isomorphism.

So in some sense, two-sided ideals play the same role as normal subgroups. That is, R/I makes sense as a ring.

18.3 Quotient ring

Definition 18.12. Given a two-sided ideal $I \subseteq R$, define an equivalence relation on R as follows:

$$a \sim b \quad \Leftrightarrow \quad a = b + x \text{ for some } x \in I$$

The functions

$$\begin{aligned} + &: R/I \times R/I \to R/I; \quad ([a],[b]) \mapsto [a+b], \\ \times &: R/I \times R/I \to R/I; \quad ([a],[b]) \mapsto [ab] \end{aligned}$$

give R/I the structure of a ring. This is called the **quotient ring**.

We really need to verify that these maps are well-defined, and satisfy the axioms of a ring. We know from our group theory that R/I with $+$ is a well-defined abelian group. So let us check that $\times$ is well-defined.

Lemma 18.13. *$\times$ is well-defined.*

Proof. Fix $a' \in [a]$ and $b' \in [b]$. We need to show that $[a'b'] = [ab]$. We know that $a' = a + x$ and $b' = b + y$ for some $x, y \in I$. Then

$$a'b' = (a+x)(b+y) = ab + xb + ay + xy.$$

But I is a two-sided ideal and $x, y \in I$. This shows that $xb, ay, xy \in I$ and so $xb + ay + xy \in I$. This shows that $a'b' \in [ab]$. □

Theorem 18.14. *$(R/I, +, \times)$ is a ring, and the function*

$$R \to R/I; \quad a \mapsto [a]$$

is a ring homomorphism.

Proof. We know that $(R/I, +)$ is an abelian group. For associativity, we can check

$$[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c].$$

For distributivity, you can do this. □

19 October 20, 2017

Last time we defined the notion of a ring homomorphism $\phi : R \to S$. These are the maps that respects addition, multiplication, and sends 1 to 1. We also talked about what a subset $I \subseteq R$ to be an ideal. An (additive) subgroup $I \subseteq R$ is called a left ideal if $x \in I$ and $r \in R$ implies $rx \in I$, and is called a right ideal if $x \in I$ and $r \in R$ implies $xr \in I$. It is two-sided if it is both left and right.

We also defined quotient rings. If $I \subseteq R$ is a two-sided ideal, we can define

$$R/I = \{[x]\} \text{ with } x \sim y \text{ if } x - y \in I.$$

This is a ring, with multiplication $[x][y] = [xy]$.

Theorem 19.1. *The function*

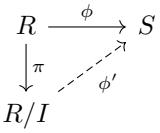
$$\pi : R \to R/I; \quad x \mapsto [x]$$

is a ring homomorphism.

Proof. We already know that this is a group homomorphism. We further see that $1 \mapsto [1]$, and also $[xy] = [x][y]$. □

19.1 Universal property and first isomorphism theorem

Corollary 19.2 (Universal property of quotient rings)**.** *Fix $\phi : R \to S$ be a ring homomorphism, and assume that $I \subseteq \ker(\phi)$ is a two-sided ideal. Then there exists a unique ring homomorphism $\phi' : R/I \to S$ such that $\psi' \circ \pi = \phi$.*



Proof. We already know from group theory that there is a unique group homomorphism ϕ'. So we only need to show that ϕ' is a ring homomorphism. This map is given by

$$\phi'([x]) = \phi(x).$$

(This is well-defined as we've shown this when we studied groups.) Then

$$\phi'([x][y]) = \phi'([xy]) = \phi(xy) = \phi(x)\phi(y) = \phi'([x])\phi'([y]).$$

Also, $\phi'([1]) = \phi(1) = 1$. □

Corollary 19.3 (First isomorphism theorem)**.** *The natural map $R/\ker(\phi) \to \operatorname{im}(\phi)$ is a ring isomorphism.*

Proof. By the universal property for quotient rings, there is such a ring homomorphism. By the first isomorphism theorem for groups, the map should be bijective. □

Example 19.4. Let $I = n\mathbb{Z} \subseteq \mathbb{Z}$ be an ideal of $\mathbb{Z}$. Then the theorem says that $R/I = \mathbb{Z}/n\mathbb{Z}$ is a ring. What is this? Denote, for $a \in \mathbb{Z}$, $[a] \in \mathbb{Z}/n\mathbb{Z}$. Then

$$[a][b] = [ab].$$

Exercise 19.5. Fill the multiplication table for $\mathbb{Z}/4\mathbb{Z}$. (By multiplication, I mean multiplication in the ring structure, not group multiplication!)

$\times$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Table 4: Multiplication table of $\mathbb{Z}/4\mathbb{Z}$

So you sometimes get two nonzero stuff multiplying to get zero.

Example 19.6. Let R be a ring and define

$$R[x]/(x^n) = \left\{ \sum_{0 \le i < n} a_i x^i \right\}.$$

Addition is just usual addition, and multiplication is given by

$$\left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{j=0}^{n-1} b_j x^j\right) = \sum_{k=0}^{n-1}\left(\sum_{i+j=k} a_i b_j\right)x^k.$$

So you just forget all the monomials over x^n. For instance, $x^a \cdot x^{n-a} = 0$.

19.2 Integral domains and fields

These rings are annoying. (Well actually these are really cool rings, but it depends on you perspective.) So we would like to make a definition that prevents this.

Definition 19.7. Let R be a commutative ring. We say that R is an **integral domain** if, whenever $xy = 0$, either $x = 0$ or $y = 0$.

The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all integral domains.

Exercise 19.8. If R is an integral domain, then $R[x]$ is also an integral domain.

Proof. Recall that the **degree** of a polynomial is the largest integer $d \in \mathbb{Z}$ for which $a_d x^d$ is nonzero. (If the polynomial is the zero polynomial, we will say that $\deg = -\infty$.)

Then $\deg(fg) = \deg(f) + \deg(g)$, if R is an integral domain. Why is this? There is the term $a_{\deg f} x^{\deg f} \cdot b_{\deg g} x^{\deg g}$. This is not zero because $a_{\deg f} b_{\deg g} \neq 0$, and it cannot be canceled about anything else. $\square$

The ring $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is a prime number.

Definition 19.9. Let R be a commutative ring, and assume $0 \neq 1$. We call R a **field** if for all $x \neq 0$, there exists a y such that $xy \neq 1$.

This is equivalent to saying that R is commutative, $0 \neq 1$, and $R^\times = R \setminus \{0\}$. Now what are some questions you might be interested in at this stage?

(1) We have G/H and R/I, and are there "quotient fields"?

(2) Are there "a lot" of finite fields?

(3) What's a "field homomorphism"?

(4) Can we turn a commutative ring R into a field by "adding inverses"?

(5) What if we look at something like

$$\left(\sum a_i x^i\right)\left(\sum b_i x^j\right) = \sum_{i,j} a_i b_j x^{(i+j) \bmod n}?$$

(6) Why are we talking only about commutative rings?

Let me start with (1) and (3). Fields are rings with some additional structure. So quotients are just quotients of rings, and field homomorphisms are ring homomorphisms. It turns out that there aren't many ideals of a field. For (2), you can classify all finite fields. The order determines the field, and you will study this in the sequel to this course. For (4), you will be able to answer this if you can answer how on earth in human history did people come up with $\mathbb{Q}$ from $\mathbb{Z}$. There is a way of doing this.

Another natural question, are there special classes of ideals such that the quotient ring has some nice property?

Definition 19.10. Let R be a commutative ring. An ideal $I \subseteq R$ is called a **prime** if $I \neq R$ and $xy \in I$ implies $x \in I$ and $y \in I$.

Definition 19.11. Let R be a commutative ring. An ideal $I \subseteq R$ is called **maximal** if $I \neq R$ and if $I \subseteq J \neq R$ is another ideal then $I = J$.

Theorem 19.12. *I is prime if and only if R/I is an integral domain, and I is maximal if and only if R/I is a field.*

20 October 23, 2017

Last time we talked about ideals and defined prime ideals and maximal ideals.

20.1 Prime ideals and integral domains

Definition 20.1. Let R be a commutative ring. Then $I \subseteq R$ is called an **ideal** if $I \subseteq (R, +)$ is a subgroup and $rx \in I$ for all $r \in R$ and $x \in I$.

Definition 20.2. Let R be a commutative ring. An ideal $I \subseteq R$ is called **prime** if for every $xy \in I$, either $x \in I$ or $y \in I$.

The name prime suggests that it has something to do with prime numbers.

Exercise 20.3. Show that $n\mathbb{Z} \subseteq \mathbb{Z}$ is a prime ideal if and only if n is prime or $n = 0$.

Solution. Assume that $x, y \in \mathbb{Z}$ such that $xy \in p\mathbb{Z}$ with p prime. Then xy is divisible by p and so either x or y is divisible by p. That is, either x or y is in $p\mathbb{Z}$. Also, it is clear that $xy = 0$ implies either $x = 0$ or $y = 0$.

Now assume that $n\mathbb{Z}$ is prime, with $n \neq 0$. If $n = ab$ composite, so that $n = ab$ with $|a|, |b| \geq 2$, then $ab \in n\mathbb{Z}$ but $a, b \notin n\mathbb{Z}$. □

Definition 20.4. A commutative ring R is is called an **integral domain** if R has no zero divisors.

Definition 20.5. An element $x \in R$ is a **zero divisor** if there exists a $y \neq 0$ in R such that $xy = 0$.

Theorem 20.6. *Let R be a commutative ring with $I \subseteq R$ an ideal. The following are equivalent:*

(1) I is prime.

(2) R/I is a non-zero integral domain.

Why don't you prove this as an exercise?

Solution. Let us first prove (1) $\Rightarrow$ (2). By definition of $R/I = \{x\}$, we have have $[x] = [0]$ if and only if $x \in I$. First we check that $I \neq R$ so R/I is not the zero ring. To show that R/I is a non-zero integral domain, we need to show that if $[x][y] = [0]$ then $[x] = [0]$ or $[y] = [0]$. We have $[x][y] = [xy]$ so

$$[x][y] = [0] \quad \Leftrightarrow \quad [xy] = [0] \quad \Leftrightarrow \quad xy \in I.$$

Because I is prime, this implies $x \in I$ or $y \in I$, so $[x] = [0]$ or $[y] = [0]$.

For the converse (2) $\Rightarrow$ (1), we can just trace back the same proof. $I \neq R$ since R/I is nonzero, and then $xy \in I$ implies $x \in I$ or $y \in I$ just means that $[x][y] = [0]$ implies $[x] = [0]$ or $[y] = [0]$. □

This fact is used all over commutative algebra, the study of commutative rings.

I also made some other definitions.

Definition 20.7. Let R be a commutative ring. An ideal $I \subseteq R$ is called **maximal** if whenever I' is an ideal such that $I \subseteq I'$, either $I' = R$ or $I' = I$.

Definition 20.8. A commutative ring R is called a **field** if $0 \neq 1$ and every $x \neq 0$ has a multiplicative inverse.

Theorem 20.9. *Fix $I \subseteq R$ an ideal and R commutative ring.*

(1) I is a maximal ideal.

(2) R/I is a field.

Before proving this, let's talk more about ideals.

20.2 Properties and constructions of ideals

Exercise 20.10. Fix and ideal $I \subseteq R$ of a commutative ring R. The following are equivalent:

(1) $I = R$.

(2) $1 \in I$.

(3) there exists some multiplicative unit $u \in I$.

(4) R/I is isomorphic to the zero ring.

Solution. It is straight-forward that (1) $\Rightarrow$ (2) $\Rightarrow$ (3). Now (3) $\Rightarrow$ (2) is because if $u \in I$ then $1 = vu \in I$. (2) $\Rightarrow$ (1) is because for any $x \in R$, $x = x \cdot 1 \in I$.

Now we prove equivalence between (1) and (4). If (1), then $[0] = [x]$ for all $x \in R$ because $x = 0 + x$. So there is only one equivalence class. If (4), then $[0] = [x]$ and so $x \in I$ for all $x \in R$. □

Proposition 20.11. *Let $I, J \subseteq R$ be ideals. Then $I \cap J \subseteq R$ is an ideal.*

We talk about ideals generated by a single element.

Proposition 20.12. *Fix $x \in R$ an element and an ideal $I \subseteq R$. The following are equivalent:*

(0) I consists of all "sums and products with x".

(1) $I = \{rx : r \in R\}$

(2) Let $\mathcal{J} = \{J \text{ ideals with } x \in J\}$. Then $I = \bigcup_{J \in \mathcal{J}} J$.

(3) $x \in I$ and if J is an ideal containing $x \in J$, then $I \subseteq J$,

Definition 20.13. For $x \in R$, R commutative, the ideal generated by x is denoted (x), and

$$(x) = \{rx : r \in R\} = \bigcap_{J \in \mathcal{J}} J.$$

Example 20.14. Let $R = \mathbb{Z}$. Then $(0) = \{0\}$ and $(n) = n\mathbb{Z}$.

Exercise 20.15. Fix R a commutative ring. The following are equivalent:

(1) R is a field.

(2) R has exactly two ideals.

Solution. Let us first prove (1) $\Rightarrow$ (2). If R is a field, then $R \neq \{0\}$ so $(0), R \subseteq R$ are distinct ideals. Now we need to show that these are the only ideals. Assume $I \subseteq R$ is an ideal such that $I \neq (0)$. Then there exists some $x \neq 0$ in I, and because R is a field, x is a unit. The previous exercise shows that $I = R$.

For (2) $\Rightarrow$ (1), we again note that $R \neq \{0\}$ because there two ideals, and then $R, (0) \subseteq R$ are two ideals. So these are all the ideals. This means that for any $x \neq 0$, we have $(x) = R$. Then $1 \in (x)$ and there exists a $y \in R$ such that $xy = 1$. □

So far this has been very abstract. I'd like to show how powerful this is.

Theorem 20.16. *Let $\mathbb{K}$ be a field. (For instance, $\mathbb{K} = \mathbb{R}$ or $\mathbb{Q}$.) Let $f \in \mathbb{K}[x]$ be an irreducible polynomial (like $f = x^2 + 1$ over $\mathbb{R}$). Then (f) is a maximal ideal, and*

$$\mathbb{K}[x]/(f)$$

is a new field, and this can be thought of as adjoining a new root of f to $\mathbb{K}$. For instance, $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

21 October 25, 2017

Last time we proved

Theorem 21.1. *Fix any commutative ring R and an ideal I. Then I is a prime ideal if and only if R/I is an integral domain.*

21.1 Maximal ideals and fields

We also had the similar theorem we haven't proven. Recall that I is maximal if $I \subseteq J$ implies $I = R$ or $I = J$. A ring R is a field if $R \neq 0$ and every nonzero $x \in R$ has a multiplicative inverse.

Theorem 21.2. *Fix any commutative ring R and an ideal I. Then I is a maximal ideal if and only if R/I is a field.*

We did the following exercise last time.

Exercise 21.3. Let $\mathbb{K}$ be a ring. Then $\mathbb{K}$ is a field if and only if $\mathbb{K}$ has exactly two ideals (0) and $\mathbb{K}$.

Also, recall from homework the following fact. For $H \lhd G$, let $\pi : G \to G/H$ be the projection map. There is a bijection

$$\left\{\begin{matrix}\text{subgroups } H' \subseteq G \\ \text{with } H \subseteq H'\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\text{subgroups} \\ L \subseteq G/H\end{matrix}\right\},$$

given by H' corresponding to $\pi(H')$ and L corresponding to $\pi^{-1}(L)$. There is an analogous statement for ideals.

Proposition 21.4. *Let R be a commutative ring and $I \subseteq R$ be an ideal. Let $\pi : R \to R/I$ be the projection map sending x to $[x]$. Then*

$$\left\{\begin{matrix}\textit{ideals } I' \subseteq R \\ \textit{with } I \subseteq I'\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\textit{ideals} \\ J \subseteq R/I\end{matrix}\right\}; \quad I' \mapsto \pi(I')$$

is a bijection.

Exercise 21.5. Prove Theorem 21.2 assuming Proposition 21.4 and Exercise 21.3.

Solution. Let's say we have a maximal ideal I. This means that there are two ideals $I' \subseteq R$ with $I \subseteq R'$. (These are $I' = I$ and $I' = R$). By the Proposition 21.4, this is equivalent to that there exists two ideals in R/I. By Exercise 21.3, this holds if and only if R/I is a field. □

Proof of Proposition 21.4. We need to show that if I' is an ideal then $\pi(I')$ is an ideal. Why is this? Any element in $\pi(I')$ can be represented as $[x]$ with $x \in I'$. For ever $[a] \in R/I$, we have

$$[a][x] = [ax] \in \pi(I')$$

because $ax \in I'$. Likewise, if $J \subseteq R/I$ is and ideal, then $\pi^{-1}(J)$ is an ideal. I'm going to leave the proof to you.

You also need to check that these maps are bijections. This can be done by showing that $\pi(\pi^{-1}(J)) = J$ and $\pi^{-1}(\pi(I')) = I'$ for all $J \subseteq R/I$ and $I \subseteq I' \subseteq R$. □

21.2 Modules

Starting from today, I am going to do linear algebra over R.

Definition 21.6. Fix a ring R. A **left module over** R is the data of

- M an abelian group
- a function $\mu : R \times M \to M$

such that for all $r, s \in R$ and $x, y \in M$,

- $(r + s)x = rx + sx$
- $r(sx) = (rs)x$
- $1x = x$
- $r(x + y) = rx + ry$.

Example 21.7. Let $R = \mathbb{R}$ and $M = \mathbb{R}^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{R}\}$. Define

$$\mu : \mathbb{R} \times M \to M; \quad (t, \vec{x}) = t\vec{x} = (tx_1, \ldots, tx_n).$$

Then you can check that all conditions are satisfied.

Definition 21.8. Let $\mathbb{K}$ be a field. A (left) module over $\mathbb{K}$ is called a **vector space** over $\mathbb{K}$.

You can define right modules similarly, and if R is commutative, the notion of a right R-module agrees with the notion of a left R-module.

Example 21.9. Let R be a ring (not necessarily commutative). Let $I \subseteq R$ be a left ideal. Then I is naturally a left R-module. This is because $R \times I \to I$ maps (a, x) to ax.

So this notion of a module includes the notion of a vector space and the notion of an ideal. Grothendieck would call this "unity".

Example 21.10. R is a left-module over itself.

Definition 21.11. Let M and N be left R-modules. Then their **direct sum** is

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

with the group structure

$$(m, n) + (m', n') = (m + m', n + n'), \quad a(m, n) = (am, an).$$

Example 21.12. Let R be a ring. Then the **free left R-module on n generators** is

$$R^{\oplus n} = R \oplus R \oplus \cdots \oplus R = R \times \cdots \times R.$$

Note that if M is a left R-module, for every $r \in R$ we have a function $M \to M$ given as $x \mapsto rx$. This is a group homomorphism, and so is an element of $\mathrm{End}(M, M)$. So we get a function

$$R \to \mathrm{End}(M, M); \quad r \mapsto (x \mapsto rx).$$

In the homework you will show that a left R-module structure on M is the same thing as a ring homomorphism $R \to \mathrm{End}(M, M)$.

This is also a really convenient way to think about modules. For instance, given an abelian group M, how many ways can we give a $\mathbb{Z}$-module structure on M? This is the same thing as a ring homomorphism

$$\mathbb{Z} \to \mathrm{End}(M).$$

You have shown in you homework that there is always a unique ring homomorphism from $\mathbb{Z}$ to any ring. So there is a unique $\mathbb{Z}$-module structure on M!

What is this module structure on M concretely? This is going to be

$$\mathbb{Z} \times M \to M; \quad (a, x) \mapsto ax$$

where ax means adding x to itself a many times.

21.3 Homomorphisms, submodules, and quotients

Let's play this natural questions game again.

- What are "submodules"?
- How do you construct "quotient modules"?
- What are linear functions? Is there a notion of homomorphisms between modules?

Definition 21.13. Let M and N be left R-modules. An **R-module homomorphism** is a function $\phi : M \to N$ such that

(1) ϕ is a group homomorphism: $\phi(x + y) = \phi(x) + \phi(y)$

(2) $\phi(ax) = a\phi(x)$.

Example 21.14. When $R = \mathbb{R}$, $M = \mathbb{R}^m$, $N = \mathbb{R}^n$, an $\mathbb{R}$-module homomorphism $M \to N$ are just linear maps from M to N.

Definition 21.15. A (left) **submodule** is a subgroup $M' \subseteq M$ such that for all $x \operatorname{im} M'$ and $a \in R$, $ax = M'$.

The word "scaling" for multiplication μ can be misleading. Let $R = \mathbb{Z}$ and

$$M = \mathbb{Z}/n\mathbb{Z} = \{\underline{0}, \underline{1}, \ldots, \underline{n-1}\}.$$

For $n \in \mathbb{Z}$ what is the scaling $n \cdot \underline{1}$? By definition,

$$n \cdot \underline{1} = \underline{1} + \cdots + \underline{1} = \underline{0}.$$

So you can scale a nonzero element to get a zero vector.

Definition 21.16. Given any submodule $M' \subseteq M$, we cendow

$$M/M' = \{[x] : x \in M\}$$

with the module structure $a[x] = [ax]$. This is called the **quotient module**.

22 October 27, 2017

Last time we defined a module. For a fixed ring R, a left module over R is the data of an abelian group M with a map $\mu : R \times M \to M$ satisfying, for all $r, s \in R$ and $x, y \in M$,

$$r(x+y) = rx + ry, \quad (sr)x = s(rx), \quad 1x = x, \quad (r+s)x = rx + sx.$$

Exercise 22.1. Let M be a left R-module. Show that

(i) $0 \cdot x = 0$

(ii) $(-1) \cdot x = -x$.

Solution. (i) We have $0x = (0+0)x = 0x + 0x$ and so $0x = 0$.

(ii) Because $0 = 0x = (1 + (-1))x = 1x + (-1)x = x + (-1)x$, we get $(-1)x = -x$. □

22.1 Linear algebra over R

Definition 22.2. Fix a ring R. The free (left) R-module on n generators is

$$R^{\oplus n} = R \times \cdots \times R$$

where

$$\mu : R \times R^{\oplus n} \to R^{\oplus n}; \quad (r, (x_1, \ldots, x_n)) \mapsto (rx_1, \ldots, rx_n).$$

Theorem 22.3. *Fix a commutative ring R. Then there exists a ring isomorphism*

$$\mathcal{M}_{n\times n}(R) \cong \mathrm{Hom}_{R-\mathsf{Mod}}(R^{\oplus n}, R^{\oplus n}) = \mathrm{End}_{R-\mathsf{Mod}}(R^{\oplus n}),$$

where $\mathcal{M}_{n\times n}(R)$ is the ring of $n \times n$ matrices with entries in R.

Why would some theorem like this useful? We can translate matrices into endomorphisms, and vice versa. Sometimes carrying out computations with matrices is more convenient and sometimes working with functions is more convenient. We can also check whether an endomorphism is invertible by looking at the determinant.

Definition 22.4. Fix an R-module M, and let $X \subseteq M$ be a subset. We say that X **spans** M if for all $y \in M$, there exist $x_1, \ldots, x_n \in X$ and $r_1, \ldots, r_n \in R$ such that

$$y = r_1x_1 + \cdots + r_nx_n = \sum_{i=1}^{n} r_ix_i.$$

We say that X is **linearly independent** if for all pairwise distinct $x_1, \ldots, x_n \in X$, whenever

$$\sum_{i=1}^{n} r_ix_i = 0 \in M,$$

then $r_i = 0$ for all i. The subset X is called a **basis** for M if X is both spanning and is linearly independent.

If you have taken linear algebra, you might be used to the fact that every module has a basis. This is very false for modules. For instance, take the $\mathbb{Z}$-module $M = \mathbb{Z}/k\mathbb{Z}$ for $k \geq 2$. Here, $k\underline{1} = 0$, so $\{\underline{1}\}$ is not linearly independent. In fact, it has no basis.

Proposition 22.5. *The module $R^{\oplus n}$ has a basis $X = \{e_1, \ldots, e_n\}$ where $e_i = (0, \ldots, 0, 10, \ldots, 0)$.*

Proof. X spans because for any $y = (y_1, \ldots, y_n) \in R^{\oplus n}$,

$$y = y_1 e_1 + \cdots + y_n e_n.$$

Conversely, if $\sum a_i e_i = 0$ then

$$0 = \sum a_i e_i = (a_1, \ldots, a_n)$$

so $a_i = 0$ for all i. □

Proposition 22.6. *Fix an R-module M. Then*

(1) any R-module homomorphism $\phi : R^{\oplus n} \to M$ is determined by $\phi(e_i)$ for $i = 1, \ldots, n$, and

(2) conversely, any choice $x_1, \ldots, x_m$ determines a unique R-module homomorphism with $\phi(e_i) = x_i$.

Proof. (1) Since $\{e_1, \ldots, e_n\}$ spans, any $y \in R^{\oplus n}$ can be written as $y = \sum_{i=1}^n y_i e_i$. So we get

$$\phi(y) = \sum_{i=1}^n \phi(y_i e_i) = \sum_{i=1}^n y_i \phi(e_i).$$

(2) Given $x_1, \ldots, x_n \in M$, note that the expression $y = \sum y_i e_i$ is unique because $\{e_1, \ldots, e_n\}$ is linearly independent. So define $\phi(y) = \sum y_i x_i$ is well-defined. □

22.2 Matrices are endomorphisms

Recall that

$$\mathcal{M}_{n\times n}(R) = \{(a_{11}, \ldots, a_{nn}) : a_{ij} \in R\} = \{(a_{ij})_{1\leq i,j\leq n} : a_{ij} \in R\}.$$

The multiplication on this is given by the following formula: if $A = (a_{ij})$ and $B = (b_{ij})$ then

$$(BA)_{ij} = \sum_{k=1}^n B_{ik} A_{kj}.$$

Proof of Theorem 22.3. By the proposition, any R-module homomorphism ϕ is determined (uniquely) by where ϕ sends $e_1, \ldots, e_n$. So define

$$\alpha : \mathcal{M}_{n\times n} \to \mathrm{Hom}_{R-\mathsf{Mod}}(R^{\oplus n}, R^{\oplus n}); \quad A = (a_{ij}) \mapsto \alpha(A) : e_i \mapsto \sum_{j=1}^{n} a_{ji} e_j.$$

This is clearly going to be a bijection. The only hard part is to show $\alpha(BA) = \alpha(B) \circ \alpha(A)$.

Because e_i form a basis and both $\alpha(BA)$ and $\alpha(B) \circ \alpha(A)$ are R-module homomorphisms, it suffices to show that $\alpha(BA)(e_i) = \alpha(B)(\alpha(A)(e_i))$. Here

$$\alpha(BA) : e_i \mapsto \sum_{j=1}^{n} (BA)_{ji} e_j = \sum_{j=1}^{n} \left(\sum_{k=1}^{n} b_{jk} a_{ki} \right) e_j.$$

On the other hand,

$$\alpha(A) : e_i \mapsto \sum_{j=1}^{n} a_{ji} e_j$$

and

$$\alpha(B) : \sum_{j=1}^{n} a_{ji} e_j \mapsto \sum_{j=1}^{n} a_{ji} \sum_{k=1}^{n} b_{kj} e_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} b_{kj} a_{ji} \right) e_k.$$

Then $\alpha(BA)$ and $\alpha(B) \circ \alpha(A)$ both maps e_j to the same vector. $\square$

23 October 30, 2017

Last time, for an R-module M, we defined some properties of a subset. We said that a subset $X \subseteq M$ is **spanning** if for all $y \in M$ there exists a finite collection $x_1, \dots, x_n \in X$ and $a_1, \dots, a_n \in R$ such that

$$y = \sum_{i=1}^{n} a_i x_i.$$

The subset X is called **linearly independent** if whenever

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

for some $x_1, \dots, x_n \in M$ with $x_i \neq x_j$ for $i \neq j$, we have $a_1 = \cdots = a_n = 0$ in R. A subset X is called a **basis** if it is both spanning and linearly independent.

Proposition 23.1. *Let $M = R^{\oplus n}$. Then any R-module homomorphism*

$$\phi : R^{\oplus n} \to N$$

is uniquely determined by $\phi(e_i)$ for $i = 1, \dots, n$.

Theorem 23.2. *Fix a commutative ring R. There exists a ring isomorphism*

$$\mathcal{M}_{n\times n}(R) \to \mathrm{End}_{R-\mathsf{Mod}}(R^{\oplus n}); \quad A = (a_{ij}) \mapsto \left(e_i \mapsto \sum_{j=1}^{n} a_{ji} e_j\right).$$

Proof. Last time we showed that this map is a ring homomorphism. Why is it injective? If some matrix is mapped to $0 \in \mathrm{End}_{M-\mathrm{Mod}}(R^{\oplus n})$ then all coefficients has to be zero. So all a_{ji} has to be zero.

Why is this surjective? An endomorphism is uniquely determined by where e_i are sent to. So by the previous proposition, there is a unique matrix that represents it. □

23.1 Playing around with bases

Exercise 23.3. Let N be an R-module. Suppose N has a basis $\{x_1, \dots, x_n\}$. Exhibit an R-module isomorphism

$$R^{\oplus n} \to N.$$

Solution. By the proposition, the assignment

$$\phi : R^{\oplus n} \to N; \quad e_i \mapsto x_i$$

is a R-module homomorphism with

$$\phi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i} r_i \phi(e_i) = \sum_{i=1}^{n} r_i x_i.$$

Let us prove the that is injective. This is because of linear independence. Because ϕ is a group homomorphism, we can just show that $\ker(\phi) = \{0\}$. But $0 = \sum_i r_i x_i$ implies $r_i = 0$ for all i by linear independence. So $\sum_i r_i e_i = 0$. On the other hand, surjectivity follows from x_i spanning. □

Exercise 23.4. let R be commutative and fix $d \in R$. Let

$$D = dI_{n\times n} = \begin{pmatrix} d & & 0 \\ & \ddots & \\ 0 & & d \end{pmatrix} \in \mathcal{M}_{n\times n}(R),$$

i.e., $D_{ij} = d$ if $i = j$ and $D_{ij} = 0$ if $i \neq j$. Show that for all $A \in \mathcal{M}_{n\times n}(R)$, we have $DA = AD$.

Solution. We can just expand both sides. First

$$(DA)_{ij} = \sum_{k=1}^{n} D_{ik}A_{kj} = D_{ii}A_{ij} = dA_{ij}$$

and next

$$(AD)_{ij} = \sum_{k=1}^{n} A_{ik}D_{kj} = A_{ij}D_{jj} = da_{ij}.$$ □

23.2 Determinant and the inverse matrix

I want to prove the following.

Theorem 23.5. *Let R be commutative. Fix some $A \in \mathcal{M}_{n\times n}(R)$. Then* $\det(A)$ *is a unit in R if and only if A is invertible.*

Example 23.6. Consider

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

which can be thought of as a map $\mathbb{Z}^{\oplus 2} \to \mathbb{Z}^{\oplus 2}$. But in this case, $\det(A) = 2 - 0 = 2$ is not a unit in $\mathbb{Z}$. So A is not invertible.

Example 23.7. Here is a dumber example. The 1×1 matrix $A = (2)$ sends $n \mapsto 2n$ from $\mathbb{Z} \to \mathbb{Z}$. Because 2 is not invertible as an integer, this map $A = (2)$ is not invertible. So we're not insane.

Definition 23.8. Let $A \in \mathcal{M}_{n\times n}(R)$, we define the (i,j)th cofactor matrix of A to be

$$\mathrm{Cof}(A)_{i,j} = \begin{pmatrix} \text{the } (n-1)\times(n-1)\text{-matrix} \\ \text{obtained by deleting} \\ i\text{th row and } j\text{th column of } A \end{pmatrix}.$$

For example, if A is 3×3 then

$$\mathrm{Cof}(A)_{2,3} = \begin{pmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{pmatrix}.$$

Definition 23.9. Let $A \in \mathcal{M}_{n\times n}(R)$. If $n = 1$, we define its **determinant** as $\det(A) = A_{11}$. Inductively, if $A \in \mathcal{M}_{n\times n}(R)$ with $n > 1$, we define

$$\det(A) = \sum_{j=1}^{n} (-1)^{1+j} A_{1j} \det(\mathrm{Cof}(A)_{1,j}) \in R.$$

Theorem 23.10 (Facts about determinants)**.** *Fix R a commutative ring.*

(1) $\det(AB) = \det(A)\det(B)$.

(2) $\det : \mathcal{M}_{n\times n}(R) \to R$ *is the unique function such that*

- $\det(I_{n\times n}) = 1$,
- det *is R-linear in each column, and*
- *if you swap two columns, the sign of the determinant changes.*

(3) For any $1 \le i \le n$,

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} A_{ij} \det(\mathrm{Cof}(A)_{i,j}).$$

I am not going to prove this here, because you might have seen this in your linear algebra class.

Example 23.11. We can compute, in $R = \mathbb{Z}/5\mathbb{Z}$,

$$\det \begin{pmatrix} 4 & 2 \\ -3 & 1 \end{pmatrix} = 4 + 6 = 0.$$

Lemma 23.12. *Given $A \in \mathcal{M}_{n\times n}(R)$, R commutative, define C as follows:*

$$C_{ij} = (-1)^{i+j} \det(\mathrm{Cof}(A)_{j,i}).$$

Then

$$AC = CA = \det(A) I_{n\times n}.$$

Proof. Fix $1 \le i \le n$. Then

$$(CA)_{ii} = \sum_{j=1}^{n} C_{ik} A_{ki} = \sum_{k} (-1)^{i+k} \det(\mathrm{Cof}(A))_{k,i} A_{ki} = \det(A).$$

For $i \neq j$, we would get

$$(CA)_{ij} = \sum_{k} C_{jk} A_{kj} = \sum (-1)^{i+j} \det(\mathrm{Cof}(A)_{k,i}) A_{kj} = \det(N),$$

where N is the matrix where entries of N equals those of A except that the ith column of N is the jth column of A:

$$N = \begin{pmatrix} \cdots & A_{*j} & \cdots & A_{*j} & \cdots \end{pmatrix}.$$

Then $\det N = 0$, and so $(CA)_{ij} = 0$. □

Using this hairy lemma, we can now prove Theorem 23.5.

Proof of Theorem 23.5. If A is invertible, then there exists a matrix B such that $AB = BA = I_{n\times n}$. Then taking determinants on both sides gives

$$\det(A)\det(B) = \det(AB) = \det(I_{n\times n}) = 1.$$

So $\det(A)$ is a unit.

Conversely, we have that $\det(A)$ is a unit. Set

$$D = (\det(A)^{-1})I_{n\times n}.$$

Then

$$(DC)A = D(CA) = D\det(A)I_{n\times n} = I_{n\times n}$$

and

$$A(DC) = A(CD) = (AC)D = \det(A)I_{n\times n}D = I_{n\times n}.$$

because $AC = CA = \det(A)I_{n\times n}$ and D commutes with any other matrix. This shows that DC is an inverse of A and A is invertible. □

24 November 1, 2017

Last time we proved:

Theorem 24.1. *Fix a commutative ring R and $A \in \mathcal{M}_{n\times n}(R)$. Then A is invertible if and only if* $\det(A)$ *is a unit in R.*

Here,

$$\det(A) = \sum_{j=1}^{n} (-1)^{1+j} A_{1j} \det(\mathrm{Cof}(A)_{1j})$$

is the unique function $\det : \mathcal{M}_{n\times n}(R) \to R$ such that

- $\det(I) = 1$,
- det is R-linear in columns,
- if A has repeating columns then $\det(A) = 0$.

Here, the third condition shouldn't be replaced with "swapping two columns changes the sign". This is because sometimes $a = -a$ with $a \neq 0$.

Exercise 24.2. Let M be a left R-module. Fix a R-module homomorphism $\phi : R^{\oplus n} \to M$. Then ϕ is an R-module homomorphism if and only if $\{\phi(e_1), \ldots, \phi(e_n)\}$ is a basis.

Solution. Last time, we saw hat if $\{v_1, \ldots, v_n\} \subseteq M$ is a basis, then $\phi(e_i) = v_i$ is an isomorphism. Assume that ϕ is an R-module isomorphism. Then ϕ is injective and so $\ker \phi = 0$. This means that

$$\phi\left(\sum_{i=1}^{n} a_i e_i\right) = \sum_{i=1}^{n} a_i \phi(e_i)$$

being zero implies $a_1 = \cdots = a_n = 0$. This just means that $\phi(e_i)$ are linearly independent.

On the other hand, ϕ is surjective. Then for any $y \in M$, there exists some a_i such that

$$\phi\left(\sum_{i=1}^{n} a_i e_i\right) = \sum_{i=1}^{n} a_i \phi(e_i) = y.$$

This means that $\phi(e_i)$ spans M. □

Corollary 24.3. *A matrix $A \in \mathcal{M}_{n\times n}(R)$ is invertible if and only if the columns of A form a basis for $R^{\oplus n}$.*

Proof. We have a ring isomorphism

$$\mathcal{M}_{n\times n}(R) \cong \mathrm{End}_{R-\mathsf{Mod}}(R^{\oplus n}).$$

Here, invertible matrices will correspond to automorphisms, i.e., isomorphisms to itself. A being invertible means that

$$\phi_A : e_i \mapsto \sum_j A_{ji} e_j$$

is invertible. By exercise, this is equivalent to $\{\phi_A(e_i)\}$ forming a basis for $R^{\oplus n}$, but $\phi_A(e_i)$ are the columns of A. □

24.1 Vector spaces have bases

But as you've seen, not all modules admit a basis. Is it a fault of the ring or the fault of the module? It's hard to say, but today I am going to show you that if the ring is a field, (finitely generated) modules admit finite bases. Also, I am going to show that they admit a well-defined *dimension*, which is a difficult concept.

Proposition 24.4. *Fix a field $\mathbb{K}$. Fix a $\mathbb{K}$-module V (i.e. a $\mathbb{K}$-vector space). Assume there exists a finite spanning set $X \subseteq V$. Then some subset of X is a basis for V.*

Proposition 24.5. *Let V be a vector space over $\mathbb{K}$. Assume $L \subseteq V$ is linearly independent, and $S \subseteq V$ is spanning. Also assume that L and S are both finite. Then*

$$|L| \leq |S|.$$

Using them, we can conclude the following.

Corollary 24.6. *Let V be a vector space over $\mathbb{K}$ and assume V can be spanned by a finite set. Then V admits a basis and given any two bases B and B', we have $|B| = |B'|$.*

Definition 24.7. We say that an R-module M is **finitely generated** if there exists a surjective R-module homomorphism

$$R^{\oplus n} \to M$$

for some n.

Definition 24.8. Let V be a finitely generated vector space over $\mathbb{K}$. The **dimension** of V is the integer $|B|$, where B is a basis for V.

Example 24.9. If V is finitely generated, V admits a finite basis by the proposition. Hence

$$V \cong \mathbb{K}^{\oplus n}$$

for some n. By the other proposition, such an n is unique.

Example 24.10. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ for $n > 0$. Then M is finitely generated but is not isomorphic to $R^{\oplus n}$ for any n.

So let us prove the two propositions.

Proof of Proposition 24.4. Given a subset $S \subseteq V$, we define

$$\mathrm{Span}(S) = \left\{ \sum_{i=1}^{n} a_i s_i : s_i \in S, a_i \in \mathbb{K}, n \geq 0 \right\}.$$

By definition $\mathrm{Span}(\emptyset) = \{0\}$.

We are going to inductively define a sequence of sets L_i. First enumerate $X = \{v_1, \ldots, v_m\}$. Let $L_0 = \emptyset$. Given L_i, let

$$L_{i+1} = \begin{cases} L_i \cup \{v_{i+1}\} & v_{i+1} \notin \mathrm{Span}(L_i) \\ L_i & v_{i+1} \in \mathrm{Span}(L_i). \end{cases}$$

Because of the following exercise, L_i being linearly independent implies L_{i+1} is also linearly independent. But $L_0 = \emptyset$ is linearly independent so all L_i are linearly independent inductively.

On the other hand, each $v_i \in \mathrm{Span}(L_i)$ for all i, and $L_i \subseteq L_m$ so $v_i \in \mathrm{Span}(L_m)$. So $\mathrm{Span}(L_m) = V$. Because L_m spans V and is linearly independent, it is a basis. □

Exercise 24.11. Suppose $L \subseteq V$ is linearly independent. If $v \notin \mathrm{Span}(L)$, then $L \cup \{v\}$ is linearly independent.

Solution. Note that if we have $\sum_i a_i v_i + av = 0$ for some $a \in \mathbb{K}$, then $a = 0$. This is because if $a \neq 0$ then

$$\sum_{i=1}^{n} \Big(-\frac{a_i}{a} \Big) v_i = v$$

contradicts $v \notin \mathrm{Span}(L)$. Since $a = 0$,

$$\sum_i a_i v_i = 0$$

and by linear independence of L, we get $a_i = 0$ for all i. This shows that $L \cup \{v\}$ is linearly independent. □

Proof of Proposition 24.5. Let $S = \{u_1, \ldots, u_m\}$ be a spanning set and $L = \{v_1, \ldots, v_n\}$ be a linearly independent set. We want to show that $m \geq n$.

Since S spans V, we can write

$$v_1 = \sum_{i=1}^{n} a_i u_i.$$

By reordering if necessary, we may assume that $a_1 \neq 0$. Dividing by a_1 then gives

$$u_1 = a_1^{-1} v_1 - \sum_{i>1} \frac{a_i}{a_1} u_i.$$

Replace v_1 by u_1, i.e., set

$$S' = \{v_1, u_2, \ldots, u_m\}.$$

This is still spanning, because u_1 is a linear combination of vectors in S'.

Now consider the projection

$$\pi : V \to V/\operatorname{Span}(v_1) = V_1$$

I claim that $\pi(S' \setminus \{v_1\})$ spans V_1 and $\pi(L \setminus \{v_1\})$ is linearly independent in V_1.

If we accept this, the result is that, in V_1, we get a set of size $m-1$ that is spanning and a set of size $n-1$ that is linearly independent. We can apply this argument repeatedly. If $m < n$, then we will get a vector space V_m such that $\emptyset$ is spanning, but some set of size $n - m > 0$ is linearly independent. But if $\emptyset$ is spanning, then $V_m = 0$. Then a nonempty set can't be linearly independent. This is a contradiction. $\square$

25 November 3, 2017

Last time we showed that "dimension is well-defined." If V is a vector space over $\mathbb{K}$, and if there is a finite spanning set, then any two bases of V have the same size. Then we define

$$\dim V = |B|.$$

This fact follows from this proposition:

Proposition 25.1. *Fix V a vector space. If S spans V and L is linearly independent in V, and S, L are finite, then $|S| \geq |L|$.*

We are going to prove this up to a claim. Suppose $S' \subseteq W$ is spanning and $L \subseteq W$ is linearly independent, and $v \in S'$, $v \in W$. Then for the projection map

$$\pi : W \to W/\mathbb{K}v,$$

$\pi(S'\{v\})$ spans $W/\mathbb{K}v$ and $\pi(L \setminus \{v\})$ is linearly independent in $W/\mathbb{K}v$. Here,

$$\mathbb{K}v = \{av : a \in \mathbb{K}\} \subseteq W$$

is a sub-vectors space (i.e., a submodule). Then we know how to take the quotient module

$$W/\mathbb{K}v = \text{module/submodule} = \{[w] : w \in W\}.$$

Let's prove the proposition given the claim.

Proof. Let $S = \{v_1, \ldots, v_m\}$ and $L = \{u_1, \ldots, u_n\}$. Last time we saw that we can replace S with

$$S' = \{u_1, v_2, \ldots, v_m\}$$

so that $\text{Span}(S') = \text{Span}(S) = V$.

Now let us use induction on m. If $m = 0$, then $V = \text{Span}(S) = \text{Span}(\emptyset) = \{0\}$. Then $L \subseteq V$ is linearly independent if and only if $L = \emptyset$. This is becuase if $L = \{0\}$ then $a \cdot 0 = 0$. This shows that $n = 0 \leq 0 = m$.

Let us assume that the statement is true for at most $m - 1$ and look at the case for m. This is assuming that if S is a spanning set and L is a linearly independent set of V, with $|S| \leq m - 1$, then $|L| \leq |S|$. If $|S| = m$, we use this fact for last time to set

$$S' = \{u_1, v_2, \ldots, v_m\}, \quad L = \{u_1, \ldots, u_n\}.$$

By the claim, $\pi(S' \setminus \{u_1\})$ is spanning in $V/\mathbb{K}u_1$ and $\pi(L \setminus \{u_1\})$ is linearly independent in $V/\mathbb{K}u_1$. On the other hand, $|S' \setminus \{u_1\}| = |S| - 1 = m - 1$. This shows that

$$|L| - 1 = |L \setminus \{u_1\}| \leq |S \setminus \{u_1\}| = |S| - 1$$

because of the inductive hypothesis. Therefore $|L| \leq |S| = m$. □

Now let us prove our claim.

Proof of Claim. We first prove that $\pi(S' \setminus \{v\})$ spans $V/\mathbb{K}v$. This means that for all $[y] \in W/\mathbb{K}v$, there exist $a_i \in \mathbb{K}$ such that

$$[y] \in \sum_{i=2}^{m} a_i[v_i],$$

where $v_i \in S'$. This means that there exist $x, x_i \in \mathbb{K}v$ such that

$$y + x = \sum_{i=2}^{m} a_i(v_i + x_i).$$

But being in $\mathbb{K}v$ is that it is a constant times v, so this is just

$$y = \sum_{i=2}^{n} a_i v_i + av$$

for some $a_i, a \in \mathbb{K}$. Every y can be expressed in this form because S is spanning.

Showing that $\pi(L \setminus \{v\})$ is linearly independent can be done similarly. Suppose there exist $a_2, \dots, a_m \in \mathbb{K}$ and $u_i \in L \setminus \{v\}$ such that

$$[0] = \sum_{i=2}^{m} a_i[u_i] \in W/\mathbb{K}v.$$

But this is just saying that

$$0 = \sum_{i=2}^{n} a_i u_i + cv.$$

Because L is linearly independent, this shows that $a_0 = 0$ for all i and $c = 0$. □

25.1 Cayley–Hamilton theorem

Fix a matrix $A \in \mathcal{M}_{n\times n}(\mathbb{R})$. What can you do with this? What are some things you've learned about matrices?

- You can look at the Jordan normal form. A matrix A has a Jordan normal form if $A \in \mathcal{M}_{n\times n}(\mathbb{K})$ where $\mathbb{K}$ is a field where all polynomial equations can be solved.
- You can look at eigenvalues or eigenvectors. This is trying to diagonalize the matrix. We want to do this because it makes it easier to study.

To get eigenvalues, we solve the **characteristic polynomial**

$$\det(A - xI) \in \mathbb{R}[x].$$

This can be generalized to arbitrary commutative rings. If $A \in \mathcal{M}_{n\times n}(R)$ with R commutative, we have $\det(A - xI) \in R[x]$.

Proposition 25.2. *Any endomorphism $\phi : R^{\oplus n} \to R^{\oplus n}$ (with R commutative) determines a ring homomorphism*

$$R[x] \to \mathrm{End}(R^{\oplus n}) \cong \mathcal{M}_{n\times n}(R)$$

by sending $x \mapsto \phi$. Then we would have

$$\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} a_i \phi^i.$$

I'm not gonna prove this proposition, but here are some examples.

Example 25.3. Let $R = \mathbb{R}$ and $\mathbb{R}^{\oplus n} = \mathbb{R}^2$. Choose $\phi = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{R}^2$. This sends

$$x \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad x^i \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}^i, \quad a_0 \mapsto \begin{pmatrix} a_0 & 0 \\ 0 & a_0 \end{pmatrix}.$$

Then we would also have stuff like

$$a_0 + x \mapsto \begin{pmatrix} a_0 + a & b \\ c & a_0 + d \end{pmatrix}, \quad a_0 x \mapsto \begin{pmatrix} a_0 a & a_0 b \\ a_0 c & a_0 d \end{pmatrix}.$$

So we have this ring homomorphism

$$R[x] \to \mathcal{M}_{n\times n}(R) = \mathrm{End}(R^{\oplus n}).$$

This can also be thought of as giving a $R[x]$-module structure on $R^{\oplus n}$.

But we have a ring homomorphism, and you can ask some questions? Is it injective? If not, what is its kernel? If $R = \mathbb{K}$ is a field, then this map cannot be injective. The reason is that $\mathbb{K}[x]$ is an infinite-dimensional vector space and $\mathcal{M}_{n\times n}(\mathbb{K})$ is finite-dimensional.

Theorem 25.4. *If $\mathbb{K}$ is a field, any ideal of $\mathbb{K}[x]$ is of the form $(f) = \{fg : g \in \mathbb{K}[x]\}$ for some $f \in \mathbb{K}[x]$.*

So if we write $\ker(R[x] \to \mathcal{M}_{n\times n}(R)) = (f)$, then $f(x) \mapsto 0$. So if we write $f(x) = \sum_i a_i x^i$ then

$$\sum_i a_i A^i = 0.$$

Theorem 25.5 (Cayley–Hamilton)**.** *Let $\det(A - xI)$ be the characteristic polynomial of $A \in \mathcal{M}_{n\times n}(R)$. Then the characteristic polynomial is in the kernel of Φ, i.e., any matrix satisfies its characteristic polynomial (or, the characteristic polynomial applied to the matrix is zero).*

Proof. Consider $A - xI \in \mathcal{M}_{n\times n}(R[x])$. There exists a map $\mathcal{M}_{n\times n}(R[x]) \to \mathcal{M}_{n\times n}(R)$. This map is defined as

$$\Psi(P) : e_i \mapsto \sum_{j=1}^{n} P_{ji}(e_j),$$

where P_{ji} is a polynomial to e_j. We'll continue next time. □

26 November 6, 2017

Last time we were proving the Cayley–Hamilton theorem.

Theorem 26.1 (Cayley–Hamilton)**.** *Fix a commutative ring R and fix $A \in \mathcal{M}_{n\times n}(R)$. Let $\det(xI - A) \in R[x]$ be the characteristic polynomial. Then A satisfies $p_A(x)$, i.e., $p_A(A) = 0$ in $\mathcal{M}_{n\times n}(R)$.*

We're actually not going to prove this and have a review session instead.

Example 26.2. Let $n = 2$. If we let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in R$, then

$$p_A(x) = \det(xI - A) = \det \begin{pmatrix} x-a & -b \\ -c & x-d \end{pmatrix} = x^2 - (a+d)x + (ad - bc).$$

Here is a cool application, although it goes slightly outside the scope of this class.

Theorem 26.3. *There does not exist an element of order 5 in $\mathrm{GL}_2(\mathbb{Z})$.*

Proof. Suppose $A^5 - I = 0$. Let us look at this ring homomorphism

$$\Phi_A : \mathbb{Z}[x] \to \mathcal{M}_{2\times 2}(\mathbb{Z}); \quad x \mapsto A.$$

This contains $x^5 - 1$ in $\ker(\Phi_A)$ by definition. On the other hand, A satisfies its own characteristic polynomial $p_A(x) \in \mathbb{Z}[x]$. So $p_A(x)$ is also in $\ker(\Phi_A)$. This isn't obvious, but this implies that $p_A(x)$ divides $x^5 - 1$, unless $A = I$ which we exclude. But it is another non-obvious fact that there is no quadratic integer polynomial divides $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$. So we get a contradiction, and this means that there cannot be any such A of order 5. □

26.1 Review session I: ideals

There are generally commutative rings and non-commutative rings. For instance, $\mathbb{Z}$ or a field $\mathbb{K}$ are commutative rings. Examples of non-commutative rings include $\mathrm{End}(A)$ or $\mathcal{M}_{n\times n}(R)$. Because of these dichotomy, there are certain adjectives you need to attach.

Definition 26.4. Fix R a ring. A **left ideal** of R is a subset $I \subseteq R$ such that

(i) I is a subgroup of $(R, +)$,

(ii) for all $r \in R$ and $x \in I$, we have $rx \in I$.

A **right ideal** can be defined similarly.

Definition 26.5. Let R be a commutative ring. Here, I is a left ideal if and only if I is a right ideal if and only if I is a two-sided ideal because the order of multiplication is commutative. Then it is simply called an **ideal**.

Definition 26.6 (and proposition)**.** In a commutative ring R, an ideal $I \subsetneq R$ is called **prime** if the following two equivalent conditions are satisfied.

(1) Whenever $xy \in I$, at least one of x or y is in I.

(2) R/I has no zero divisors.

For example, in $R = \mathbb{Z}$, $I = p\mathbb{Z} = (p)$ is a prime ideal if p is a prime number.

Definition 26.7 (and proposition again)**.** In a commutative ring R, an ideal $I \subsetneq R$ is called **maximal** if it satisfies the following two equivalent conditions.

(1) Whenever $I \subseteq J$ with J an ideal, either $I = J$ or $J = R$.

(2) R/I is a field.

In particular, every maximal ideal is a prime ideal because a field is an integral domain. Also note that in $\mathbb{Z}$ there are many maximal divisors. In fact, the only prime ideal that is not maximal is (0).

26.2 Review session II: universal properties

Let's recall what the first isomorphism theorem says.

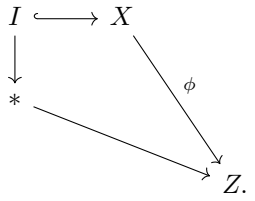
Theorem 26.8 (First isomorphism theorem)**.** *Fix a homomorphism $\phi : X \to Y$. It could be that X and Y are groups, it could be that they are rings, it could be that they are R-modules. Then the natural map*

$$X/\ker(\phi) \to \operatorname{im}(\phi) \subseteq Y$$

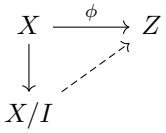
is an isomorphism.

Where does the universal property come up? The point is that there *is* a natural map.

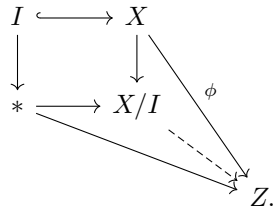
Theorem 26.9 (Universal property of quotients)**.** *Fix a homomorphism $\phi : X \to Z$. Suppose that $\ker(\phi) \supseteq I$. This can be drawn as the following commutative diagram:*



Then there exists a unique homomorphism $X/I \to Z$ making the triangle



commute. In the larger picture, we can fill in as



Here, the there are specific stuff we can quotient out by. For groups, we need $I \triangle X$ is a normal subgroup. For rings, we need that $I \subseteq X$ is an ideal. For R-modules, we need that $I \subseteq X$ is a submodule. If you don't remember, this is the definition of a submodule.

Definition 26.10. Fix a (left) R-module X. (This means that there is a multiplication map $\mu : R \times X \to X$.) A **submodule** is a subset $X' \subseteq X$ such that

(1) $X' \subseteq X$ is a (additive) subgroup,
(2) for all $r \in R$ and $x' \in X'$, we have $rx' \in X'$.

Here, if $I \subseteq X$ is such an object that we can quotient out by, we can define the quotient

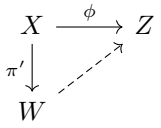
$$X/I = \{[x] : x \in X\}.$$

Here we are using the equivalence relation that $[x] = [y]$ if and only if

- $xy^{-1} \in I$, if X is a group,
- $x - y \in I$, if X is a ring or a module.

Here is an application of the universal property.

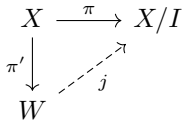
Proposition 26.11. *Suppose W satisfies the same universal property as X/I. (Here, W comes with a specified map $\pi' : X \to W$ such that $\ker(\pi') \supseteq I$.) This means that for all $\phi : X \to W$ with $\ker(\phi) \supseteq I$, there exists a unique $W \to Z$ such that*



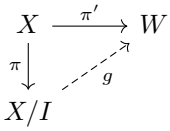
commute. Then W is isomorphic to X/I.

The nice thing is that we can prove this without writing down elements at all.

Proof. Let $Z = X/I$. By the universal property for W, we find a unique map $j : W \to X/I$ that makes

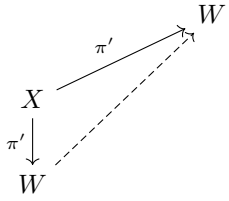


commute. Likewise, let $Z = W$ in the universal property for the quotient. Then we get a unique map $g : X/I \to W$ such that

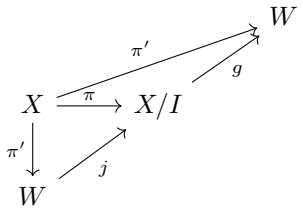


commute.

We now claim that g are inverse isomorphism. This is a nice trick. Note that letting $Z = W$ in the universal property for W gives that there is a unique dashed arrows making



commute. But the identity map id_W satisfies this, so this is the unique such map. On the other hand, the diagram



commutes. This shows that $g \circ j = \mathrm{id}_W$. The exact same argument shows that $j \circ g = \mathrm{id}_{X/I}$, and so g and j are inverse isomorphisms. □

26.3 Review session III: vector spaces, modules, and orbit spaces

Recall that in $\mathbb{R}$-vector spaces, linear transformations are defined as

Definition 26.12. A function $\phi : \mathbb{R}^m \to \mathbb{R}^n$ is called **linear** (or **$\mathbb{R}$-linear**) if

- $\phi(x, y) = \phi(x) + \phi(y)$ and

- $\phi(\lambda x) = \lambda\phi(x)$.

Module homomorphisms are exact analogues.

Definition 26.13. Let M and N be (left) R-modules. An **R-module homomorphism** (or just an **R-linear map**) is a function $\phi : M \to N$ such that

- ϕ is a group homomorphism, i.e., $\phi(x+y) = \phi(x) + \phi(y)$, and
- for all $r \in R$ and $x \in M$, we have $\phi(rx) = r\phi(x)$.

Any linear map $\phi : \mathbb{R}^m \to \mathbb{R}^n$ is determined by the elements

$$\phi \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \phi \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Proposition 26.14. *Likewise, any R-linear map $\phi : R^{\oplus m} \to R^{\oplus n}$ is determined by $\phi(e_i)$.*

A group action $G \times X \to X$ induces an equivalence relation on X, given by

$$x \sim y \quad \Leftrightarrow \quad \mathcal{O}_x = \mathcal{O}_y.$$

In this case, we have the orbit space $G \setminus X = \{\mathcal{O}\}$.

In the special case when $H \lhd G$ is a normal subgroup and the (right) action $G \times H \to G$ is given by $(g, h) \mapsto gh$, then the equivalence relation will be given by

$$g \sim g' \quad \Leftrightarrow \quad gH = g'H.$$

Then the orbit space is G/H, and there is a group structure on it.

27 November 8, 2017

We're going to do more review.

27.1 Review session IV: conjugacy classes

In the beginning of this class we studied groups. Fix a group G. There are two actions of G you can give on itself: there is the left multiplication

$$G \times G \to G; \quad (g, x) \mapsto gx,$$

and there is the conjugation

$$G \times G \to G; \quad (g, x) \mapsto gxg^{-1}.$$

The conjugation is a far more interesting action. When we act by g on e, left multiplication sends e to g, and conjugation sends e to e. So there is already a fixed point of the conjugation action. Also, the fixed points picks out precisely the center.

Proposition 27.1. *Let's say that $x \sim y$ if x and y are in the same conjugacy action. (In other words, $gxg^{-1} = y$ for some g.) This is an equivalence relation.*

Definition 27.2. The **conjugacy class** of $x \in G$, is $[x]$ under $\sim$. We can explicitly write

$$[x] = \{y : gxg^{-1} = y \text{ for some } g\}.$$

If $y = gxg^{-1}$ then x and y look interchangable. (So $\{e\}$ is the conjugacy class of e because nothing looks like the identity.) The reason for this is that

$$G \to G; \quad x \mapsto gxg^{-1}$$

is a group automorphism. So x and gxg^{-1} sort of play the same role.

The class equation is simply counting elements of G by conjugacy classes. Because conjugacy classes partition G, we have

$$G = \bigcup_{\text{conj. classes } I} I = \coprod_{\text{conj. classes } I} I.$$

If G is a finite group, we then know that

$$|G| = \sum_{\text{conj. classes } I} |I|.$$

Furthermore, the orbit-stabilizer theorem says that

$$|I| = \frac{|G|}{|G_x|}$$

where $G_x = \{g : gxg^{-1} = x\}$ is the centralizer. So you could also write

$$|G| = \sum_I \frac{|G|}{|G_x|},$$

where here you're picking some arbitrary $x \in I$ to compute G_x.

In the homework you've seen an application to finding normal subgroups of A_5. If $N \lhd G$ is a normal subgroup, then

$$N = \coprod_{\substack{\text{conj. classes} \\ I \subseteq N}} I.$$

So if you know all the sizes of conjugacy classes $|I|$, and know Lagrange's theorem that $|N|$ divides $|G|$, then you can get a lot of information.

If you don't remember how to prove orbit-stabilizer, here's how you do it. Suppose that $G \times X \to X$ is a group action. For $x \in X$, there are

Are there other automorphisms? In general, you only know the conjugation automorphisms. But if you know more information, there can be other automorphisms. Suppose A is an abelian group. Then

$$A \to A; \quad a \mapsto -a$$

is an automorphism, because $a + b \mapsto -(a + b) = -a - b$. Note that this is true because A is abelian. For a non-abelian group G,

$$(xy)^{-1} = y^{-1}x^{-1} \neq x^{-1}y^{-1}$$

so $x \mapsto x^{-1}$ is a bijection, but not a homomorphism.

The automorphisms of G coming from conjugation are called **inner automorphisms**. Recall that for each $g \in G$ we have an automorphism $x \mapsto gxg^{-1}$, and then we have a function

$$G \to \mathrm{Aut}(G); \quad g \mapsto (x \mapsto gxg^{-1}).$$

We showed that this is a homomorphism, and the image precisely the inner automorphisms. In particular, the inner automorphisms form a subgroup of $\mathrm{Aut}(G)$.

27.2 Review session V: modules and matrices

Given a ring R, a **left module** is the data of an abelian group M with a function

$$R \times M \to M$$

called scaling.

Example 27.3. If $R = \mathbb{Z}$, any abelian group A is uniquely a $\mathbb{Z}$-module. Here, the map is given by

$$\mathbb{Z} \times A \to A; \quad (n, a) \mapsto \begin{cases} \overbrace{a + \cdots + a}^{n} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{|n|} & n < 0. \end{cases}$$

So if $M = \mathbb{Z}/n\mathbb{Z}$, we have

$$n\underline{1} = \underline{1} + \cdots + \underline{1} = \underline{0}.$$

Example 27.4. For any R and $n \geq 0$, we have the free module

$$R^{\oplus n} = R \times R \times \cdots \times R$$

as an abelian group with usual addition, and scaling

$$R \times R^{\oplus n} \to R^{\oplus n}; \quad (r, (x_1, \ldots, x_n)) \mapsto (rx_1, \ldots, rx_n).$$

Other examples include ideals. But for these nice-looking free modules $R^{\oplus n}$, we can characterize its ring of R-module endomorphisms.

Proposition 27.5. *For R a commutative ring,*

$$\mathcal{M}_{n\times n}(R) \cong \mathrm{End}_{R-\mathsf{Mod}}(R^{\oplus n}).$$

When working with matrices, we can add and multiply them, and we can also check invertibility using the determinant.

Theorem 27.6. *Fix $A \in \mathcal{M}_{n\times n}(R)$. The following are equivalent:*

(1) A is invertible.

(2) $\det(A) \in R^\times$.

(3) The columns of A form a basis for $R^{\oplus n}$.

Most modules don't admit a basis. But when $R = \mathbb{K}$ is a field, modules do admit a basis. If a R-module M admits a basis, then $M \cong R^{\oplus n}$. So every (finitely generated) $\mathbb{K}$-vector space is isomorphic to some $\mathbb{K}^{\oplus n}$.

Example 27.7. If $R = \mathbb{Z}/n\mathbb{Z}$, then

$$M = (\mathbb{Z}/n\mathbb{Z})^{\oplus k} = \mathbb{Z}/n\mathbb{Z} \times \cdots \times \mathbb{Z}/n\mathbb{Z}$$

is a free module over R.

If $R = \mathbb{Z}/p\mathbb{Z}$, this is a field. So any $\mathbb{Z}/p\mathbb{Z}$-module admits a basis. This means that if V is finite, then we could always write

$$V \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus k} = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}.$$

28 November 13, 2017

Today I want to talk about the Euclidean algorithm and greatest common divisors. I want to make a definition that makes sense for all commutative rings.

28.1 Principal ideal domains

In a commutative ring R, we say that d **divides** f or $d \mid f$ if there exists some element $e \in R$ such that

$$d \cdot e = f.$$

Definition 28.1. Let R be an integral domain. Fix two elements $f, g \in R$. A **greatest common divisor** is an element $d \in R$ such that

- $d \mid f$ and $d \mid g$,
- if d' is such that $d' \mid f$ and $d' \mid g$, then $d' \mid d$.

Example 28.2. Let $R = \mathbb{Z}$ and $f = p$, $g = q$ be two distinct prime numbers. Then both 1 and -1 are greatest common divisors.

Definition 28.3. Let R be an integral domain. We say that R is a **principal ideal domain** or **PID** for short, if for all ideal $I \subseteq R$ there exists a $x \in R$ such that $I = (x)$.

Example 28.4. $R = \mathbb{Z}$ is a principal ideal domain. Any ideal is of the form $n\mathbb{Z} = (n)$.

Example 28.5. The ring $R = \mathbb{K}[t]$ is a principal ideal domain, where $\mathbb{K}$ is a field.

Fix two elements $x, y \in R$ and consider the ideal

$$I = (x, y) = \{rx + sy : r, s \in R\}.$$

If R is a principal ideal domain, there exists a $z \in R$ such that $(x, y) = (z)$.

Proposition 28.6. *Let R be a principal ideal domain, and fix $f, g \in R$. Then $(f, g) = (h)$ if and only if h is a greatest common divisor of f and g.*

If $(f, g) = (h)$ then $h \in (f, g)$ so there exist $r, s \in R$ such that

$$rf + sg = h.$$

On the other hand, $f, g \in (f, g) = (h)$ and so there exist $a, b \in R$ such that

$$f = ah, \quad g = bh.$$

Proof. We first prove that $(f, g) = h$ implies that h is a greatest common divisor. By the remark we have just made, $h \mid f$ and $h \mid g$. Now consider an $d' \in R$ such that $d' \mid f$ and $d' \mid g$. Then $f, g \in (d')$ and so $(f, g) \subseteq (d')$. This shows that

$h \in (f,g) \subseteq (d')$. Note that we have not used the fact that R is a PID in this direction.

Now Now suppose that h is a greatest common divisor for f, g. Then $h \mid f, g$ and so $f, g \in (h)$. Then $(f,g) \subseteq (h)$. On the other hand, for all d' such that $d' \mid f$ and $d' \mid g$, we get $(f,g) \subseteq (d')$. Since h is the greatest common divisor, for all such d' we have

$$(h) \subseteq (d').$$

But because R is a PID, we can choose z such that $(f,g) = (z)$. Then z is a common divisor of f and g and so

$$(f,g) \subseteq (h) \subseteq (z) = (f,g)$$

and so $(f,g) = (h)$. □

28.2 Euclidean algorithm

This algorithm is a way to produce a greatest common divisor given f and g. You can interpret this as producing a grid. Let

$$B_0 = f, \quad B_1 = g$$

in $\mathbb{Z}_{>0}$ and you are trying to measure lengths in terms of B_0 and B_1. Assume without loss of generality $B_0 > B_1$. What you can do get a shorter length than B_1 is to take away B_1s from B_0. Then you will end up with some length B_2 less than B_1.

$$B_0 = a_1 B_1 + B_2, \quad B_2 < B_1$$

If we want a length smaller than B_2, then we can also do the same thing with B_1 and B_2. Consider B_1 and take away B_2 from it to get the length $B_3 < B_2$.

$$B_1 = a_2 B_2 + B_3, \quad B_3 < B_2$$

Repeating this will give

$$B_i = a_{i+1} B_{i+1} + B_{i+2}, \quad B_{i+2} < B_{i+1}$$

and this stops at some $B_{n-1} = a_n B_n + 0$ because the length can't be between 0 and 1.

Here is a formal way to write this. Given any $R \in R$, suppose we have a notion of "size" σ, such that $\sigma(B)$ is a positive integer unless $B = 0$ in which case $\sigma(0) = 0$. For example, $R = \mathbb{Z}$ and $\sigma(B) = |B|$ is something we want. We also assume that for any two $B_0, B_1 \in R$, we can find $a_1 \in R$ such that

$$B_0 = a_1 B_1 + B_2, \quad \sigma(B_2) < \sigma(B_1).$$

Definition 28.7. An integral domain R equipped with a size function $\sigma : R \to \mathbb{Z}_{\geq 0}$, satisfying the "formal structure" is called a **Euclidean domain**.

Proposition 28.8. *Let R be a Euclidean domain. Fix $B_0, B_1 \in R$. Let B_n be "the end" of the Euclidean algorithm:*

$$B_{n-1} = a_n B_n + 0$$

Then B_n is a greatest common divisor of B_0 and B_1.

The strategy is to prove that $(B_0, B_1) = (B_n)$.

Lemma 28.9.

(a) For all $0 \leq j \leq n$, $B_{n-j} \in (B_n)$.

(b) For all $0 \leq k \leq n$, $B_k \in (B_0, B_1)$.

If I could prove this, we would know that $B_0, B_1 \in (B_n)$ from (a) and then $(B_0, B_1) \subseteq (B_n)$. From (b) we would know that $B_n \in (B_0, B_1)$ and so $(B_n) \subseteq (B_0, B_1)$.

Proof. (a) For $j = 0$, we know $B_n \in (B_n)$. Now assume that it is true for all $j' \leq j$. We need to show that $B_{n-(j+1)} \in (B_n)$. But we have

$$B_{n-j-1} = a_{n-j} B_{n-j} + B_{n-j+1} \in (B_n)$$

because $B_{n-j}, B_{n-j+1} \in (B_n)$ by the inductive hypothesis.

(b) Again, the base case $k = 0, 1$ is trivially true. Assume it is true for $k' \leq k$. Now we can show that

$$B_{k+1} = B_{k-1} - a_k B_k \in (B_0, B_1)$$

because $B_{k-1}, B_k \in (B_0, B_1)$. □

28.3 Sylow subgroups

Fix a finite group G. Its order is going to be some integer

$$|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

Here we're assuming that p_i are primes, $p_i \neq p_j$ for $i \neq j$, and $n_i \geq 1$ for all i.

We know that $n \mid |G|$ for all $H \subseteq G$ with $|H| = n$. But is the converse true, i.e., if $n \mid |G|$ does there exist a subgroup $H \subseteq G$ such that $|H| = n$?

The answer is no, so maybe we can ask a weaker/simpler question. Does there exist a subgroup $H \subseteq G$ such that $|H| = p_i^{n_i}$? Or we can ask about elements of special order. Is there an element $g \in G$ such that $|g| = p_i^{n_i}$? What about $|g| \mid p_i$?

Definition 28.10. Fix $p = p_i$. A **p-Sylow subgroup** H is a subgroup of G such that $|H| = p_i^{n_i}$.

Theorem 28.11 (Sylow)**.** *p-Sylow subgroups exist for all $p = p_i$.*

Definition 28.12. Let $H \subseteq G$. Then

$$|G/H| = [G : H]$$

is called the index of H in G.

Exercise 28.13. Let $G = \mathrm{GL}_n(\mathbb{F}_p)$. Let

$$H = \{A \in \mathrm{GL}_n(\mathbb{F}_p) : A \text{ is an upper triangular matrix with } \mathrm{diag}(A) = (1, \ldots, 1)\}.$$

Then H is a p-Sylow subgroup of G.

29 November 15, 2017

Last time I stated the theorem. Let G be a finite group and p be a prime. Let p^N be the largest power of p dividing $|G|$.

Definition 29.1. A subgroup $S \subseteq G$ is called a **p-Sylow subgroup** (sometimes a **Sylow p-subgroup**) if $|S| = p^N$.

Example 29.2. For $G = S_3$, we have $|G| = 6 = 2 \cdot 3$. So the 2-Sylow subgroups are

$$\{e, (12)\}, \quad \{e, (13)\}, \quad \{e, (23)\}.$$

The 3-Sylow subgroups are

$$\{e, (123), (132)\}.$$

29.1 First Sylow theorem

Theorem 29.3 (First Sylow theorem)**.** *Fix a finite group G and a prime p. Then there exists a p-Sylow subgroup $S \subseteq G$.*

This theorem is really powerful.

Exercise 29.4. Let p be a prime dividing $|G|$. Show that there exists an element of order p in G.

Solution. Fix a p-Sylow subgroup $S \subseteq G$ so that $|S| = p^N$. Choose $x \neq e$ such that $x \in S$. Because x is an element of S, the order of x divides the order of S, which is a power of p. This shows that

$$|x| = p^k$$

for some $1 \leq k \leq N$. Then

$$(x^{p^{k-1}})^p = x^{p^k} = 1$$

and $x^{p^{k-1}} \neq e$. So $x^{p^{k-1}}$ has order p. □

Let us now try to prove the theorem. We are going to provide a large enough universal example with a p-Sylow subgroup, and then show that this implies that all groups have p-Sylow subgroups.

Exercise 29.5. Let $\underline{G} = \mathrm{GL}_n(\mathbb{F}_p)$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ as a field, and let

$$\underline{S} = \{A \in \underline{G} : A \text{ is upper-triangular and } \operatorname{diag}(A) = (1, \ldots, 1)\} = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & \end{pmatrix} \right\}.$$

Show that $\underline{S}$ is a p-Sylow subgroup of $\underline{G}$.

Solution. Note that G is in bijection with the ordered bases of $\mathbb{F}_p^{\oplus n}$. We can count its number as

$$|\underline{G}| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}).$$

This is because the first vector can be anything but zero, the second vector can by anything that is not spanned by the first one, and so on. So

$$|G| = p^{1+2+\cdots+(n-1)} \cdot (\text{sth not divisble by } p).$$

On the other hand, elements of $\underline{S}$ are of the form

$$\begin{pmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & 1 & a_{23} & \cdots & a_{2n} \\ 0 & 0 & 1 & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

and so we have p choices for each of the a_{ij} with $j > i$. This shows that

$$|\underline{S}| = p \cdot p^2 \cdot \cdots \cdot p^{n-1} = p^{1+2+\cdots+(n-1)}.$$

This shows that $\underline{S}$ is a p-Sylow subgroup. □

Now there is going to be one main lemma that gets everything going smoothly.

Lemma 29.6 (Main lemma)**.** *Let $\underline{S} \subseteq \underline{G}$ be a p-Sylow subgroup. Fix any subgroup $\underline{H} \subseteq \underline{G}$. Then there exists a $g \in \underline{G}$ such that*

$$g\underline{S}g^{-1} \cap \underline{H}$$

is a p-Sylow subgroup of $\underline{G}$.

Before we prove it, let us do an exercise.

Exercise 29.7. Let's describe $g\underline{S}g^{-1} \cap \underline{H}$ more usefully. Recall that $\underline{H}$ acts on $\underline{G}/\underline{S}$ as

$$\underline{H} \times \underline{G}/\underline{S} \to \underline{G}/\underline{S}; \quad (h, g\underline{S}) \mapsto (hg)\underline{S}.$$

Show that $g\underline{S}g^{-1} \cap H$ is the stabilizer of $g\underline{S}$ under this action.

Solution. Fix $h \in g\underline{S}g^{-1} \cap H$. Then there exists an $s \in \underline{S}$ such that $h = gsg^{-1}$. Then $hg = gs$, with the left being an element of $hg\underline{S}$ and the right being an element of $g\underline{S}$. This shows that $hg\underline{S} = g\underline{S}$. This shows that $g\underline{S}g^{-1} \cap H$ is contained in hte stabilizer.

Now suppose that h is in the stabilizer. There exist $s_1, s_2 \in \underline{S}$ such that $hgs_1 = gs_2$. Then $h = g(s_2 s_1^{-1})g^{-1}$ so h is in the intersection. □

Proof of Main lemma. Consider the group action

$$\underline{H} \times \underline{G}/\underline{S} \to \underline{G}/\underline{S}.$$

Then we have

$$\underline{G}/\underline{S} = \coprod_{\mathcal{O} \text{ orbit}} \mathcal{O}$$

and so by the orbit-stabilizer theorem,

$$\frac{|\underline{G}|}{|\underline{S}|} = |\underline{G}/\underline{S}| = \sum \frac{|\underline{H}|}{|\text{Stab of } \mathcal{O}|}.$$

Now because $\underline{S}$ is a p-Sylow subgroup of $\underline{G}$, the left hand side is not divisible by p. Thus there exists some $\mathcal{O}$ such that $|\underline{H}|/|\text{Stab}|$ is not divisible by p.

But we know something about the stabilizer. We know that

$$\text{Stab} = g\underline{S}g^{-1} \cap H$$

So $|\text{Stab}|$ divides $|g\underline{S}g^{-1}| = p^N$. So $|H|/|\text{Stab}|$ not divisible by p implies that $|\text{Stab}|$ is the highest power of p dividing $|H|$. □

This immediately implies the first Sylow theorem.

Proof of Theorem 29.3. Fix G an arbitrary finite group and p a prime. Then the Cayley theorem gives an embedding

$$j : G \hookrightarrow \text{Aut}_{\mathsf{Set}}(G) \cong S_{|G|} \hookrightarrow \text{GL}_{|G|}(\mathbb{F}_p) = \underline{G}.$$

Here, the second embedding is just given by permutation matrices. Also there is a p-Sylow subgroup $\underline{S} \subseteq \underline{G}$.

Now by the main lemma, there exists a $A \in \underline{G}$ such that

$$A\underline{S}A^{-1} \cap j(G) = H'$$

is a p-Sylow subgroup of $j(G)$. Because $j : G \to j(G)$ is an isomorphism, we can take the inverse image and get $j^{-1}(H') \subseteq G$ a p-Sylow subgroup. □

This is a common technique in math. Another way of proving this theorem is to cook up a clever conjugation on the sets of size p^N. But this is rough. This proof is somewhat different. We are making a very big example where it is not hard to check and show that this implies the smaller cases.

29.2 Second Sylow theorem

Theorem 29.8 (Second Sylow theorem)**.**

(1) Any $H \subseteq G$ such that $|H| = p^k$ is contained in a p-Sylow subgroup of G.

(2) If S, S' are p-Sylow subgroups of G, they are conjugate.

(3) The number of p-Sylow subgroups is 1 *modulo* p.

Let me give you an example of why this is powerful.

Example 29.9. Let $|G| = pq$, with $q < p$ different primes. Then either $G \cong \mathbb{Z}/pq\mathbb{Z}$ or G is isomorphic to some explicitly describable other non-abelian group with $q \mid p - 1$. You describe this group in the homework.

Proof of Theorem 29.8. (1) Let $S \subseteq G$ be a p-Sylow subgroup. By the main lemma, there exists a $g \in G$ such that

$$gSg^{-1} \cap H \subseteq H$$

is a p-Sylow subgroup. But $|H|$ is a power of p and so the only p-Sylow subgroup of H is H itself. This shows that gSg^{-1} contains H, where gSg^{-1} is a p-Sylow subgroup.

(2) Take $H = S'$ in the main lemma. Then there exists a g such that $gSg^{-1} \cap S' = S'$ and so $gSg^{-1} = S'$.

(3) This is more involved. We are going to need the following lemma and we will continue next time. □

Lemma 29.10. *Suppose $S, S' \subseteq G$ are p-Sylow, and also suppose that for all $s \in S$ we have $sS's^{-1} = S'$. Then $S = S'$.*

30 November 17, 2017

We were proving some great theorems. Recall that for a finite group G and p a prime, a subgroup $S \subseteq G$ is called a p-Sylow subgroup of G if $|S|$ is a power of p and $|G|/|S|$ is not divisible by p. If

$$|G| = p_1^{n_1} \cdots p_a^{n_a}$$

is the prime factorization, this means that $|S| = p_i^{k_i}$ if $p = p_i$ for some i, or maybe p is not in the prime factorization and $|S| = 1$.

Example 30.1. Let $G = S_4$ so that $|G| = 4! = 2^3 \cdot 3$. We showed last time that G always has a p-Sylow subgroup. So we are going to look for 2-Sylow subgroups and 3-Sylow subgroups. Can you think of a subgroup of S_4 of order 8? The symmetries of the square permutes the vertices, so we have an injective group homomorphism

$$D_8 \hookrightarrow S_4.$$

If we use the 1234 as the square, the image can listed as

$$\{e, (13), (12)(34), (14)(23), (24), (1234), (13)(24), (1432)\}.$$

But how many 2-Sylow subgroups does S_4 have, and are they all isomorphic?

Let us look at 3-Sylow subgroups. We need to look at groups of order 3, and so they should be all isomorphic to $\mathbb{Z}/3\mathbb{Z}$. They are going to be

$$\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle.$$

Definition 30.2. Fix a prime p. A group is a **p-group** if its order is a power of p.

Theorem 30.3 (Second Sylow theorem)**.**

(1) Let $H \subseteq G$ be a p-group. Then there exists a p-Sylow subgroup S such that $H \subseteq S$.

(2) Let S, T be p-Sylow subgroups of G. Then S and T are conjugates.

(3) The number of p-Sylow subgroups $S \subseteq G$ is 1 modulo p.

The third statement gives a hint for how you could count this. In the case of S_4, the 2-Sylow subgroup we found is not a normal subgroup, as conjugation is relabeling the elements. So there is at least 3 such subgroups, because the number is odd. We are going to play this game with Sylow subgroups.

Lemma 30.4. *Let S, T be two p-Sylow subgroups of G. Assume that $tSt^{-1} = S$ for all $t \in T$. Then $S = T$.*

Proof. Define

$$N(S) = \{x \in G : xSx^{-1} = S\}.$$

Then $N(S)$ is a subgroup of G. This is because (i) $eSe^{-1} = S$, (ii) $x, y \in N(S)$ implies $xySy^{-1}x^{-1} = xSx^{-1} = S$, and (iii) $x \in N(S)$ implies $x^{-1}Sx =$

$x^{-1}xSx^{-1}x = S$. Moreover, S and T are subgroup of $N(S)$. So S, T are actually p-Sylow subgroups of $N(S)$.

But observe that $S \lhd N(S)$, because we made $N(S)$ so that S is normal. By (2) of Theorem 30.3 applied to $N(S)$, there exists an $x \in N(S)$ such that $S = xSx^{-1} = T$. Therefore $S = T$. □

Proof of (3) of Theorem 30.3. Because we are dealing with finite groups, the only tool is group actions and counting. Let

$$X = \{p\text{-Sylow subgroups } S \subseteq G\}$$

and consider the conjugation action

$$T \times X \to X; \quad (t, S) \mapsto tSt^{-1}$$

of an arbitrary p-Sylow subgroup T on X. Then

$$|X| = \sum |\mathcal{O}| = \sum \frac{|T|}{|\text{Stab}|} = \sum \frac{p^N}{p^k} = 1 + \cdots + 1 + p^{a_1} + \cdots + p^{a_x},$$

where $a_i \geq 1$.

Now let us really look at what the $|T|/|\text{Stab}|$ case is. This is equivalent to $\text{Stab} = T$, which means that $\{t \in T : tSt^{-1} = S\} = T$. But the previous lemma says that this is possible only when $S = T$. Therefore there is exactly 1 and the right hand side is 1 modulo p. Therefore $|X| \equiv 1 \pmod{p}$. □

30.1 Classification of finite abelian groups

Let's apply the Sylow theorems to G abelian. We can write out its prime factorization

$$|G| = p_1^{n_1} \cdots p_a^{n_a}.$$

By the first Sylow theorem, for each p_i there exists a subgroup $H_i \subseteq G$ such that $|H_i| = p_i^{n_i}$. So we have group homomorphisms

$$\phi_i : H_i \hookrightarrow G.$$

But because G is abelian, we can take the product

$$\phi : H_1 \times H_2 \times \cdots \times H_a \to G; \quad (h_1, \ldots, h_a) \mapsto \phi_1(h_1) + \cdots + \phi_a(h_a).$$

The claim is that this is an isomorphism. Why should it be? Well first we see that the sizes match up. So we can either show that it is an injection or a surjection. The point is that H_i have relatively prime order.

Exercise 30.5. Suppose A, B are subgroups of an abelian group G, such that $\gcd(A, B) = 1$. Then the function

$$A \times B \to G; \quad (a, b) \mapsto a + b$$

is an injection.

Solution. Suppose $a + b = 0$ so that $a = -b$. Then $a \in A$ and $b = -a \in A$ so $|\langle a \rangle|$ divides $|A|$ and $|B|$. This shows that $|\langle a \rangle| = 1$ and $a = 0$. □

Corollary 30.6. *If G is a finite abelian group, then G is isomorphic to the direct product of its maximal p-groups.*

Now we are very close to classifying finite abelian groups. If we can classify all abelian p-groups, we are done.

Theorem 30.7 (Classification of abelian p-groups)**.** *Let A be an abelian group. Then there exists a unique sequence of numbers*

$$a_r \geq a_{r-1} \geq \cdots \geq a_1$$

such that

$$A \cong (\mathbb{Z}/p^{a_r}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_1}\mathbb{Z}).$$

Let us consider $p = 2$.

- There is only one group of order 2, which is $\mathbb{Z}/2\mathbb{Z}$.
- There are two groups of order 4, which are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- There are three groups or order 8, which are $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

In particular, to classify abelian group of order p^N, it suffices to write all partitions $N = a_r + \cdots + a_1$.

31 November 20, 2017

Last time we've been using the Sylow theorems to classify finite abelian groups.

Theorem 31.1 (Sylow)**.** *p-Sylow subgroups exist, and any two p-Sylow subgroups are conjugate to each other.*

Corollary 31.2. *If G is abelian, there exists a unique p-Sylow subgroup in G.*

We also showed that for a finite abelian A, the homomorphism

$$H_{p_1} \times \cdots \times H_{p_n} \to A; \quad (h_1, \ldots, h_n) \mapsto h_1 + \cdots + h_n$$

is an isomorphism. We can use this to classify finite abelian groups. Last time, we stated the fact that any abelian group of order p^N is isomorphic to

$$\mathbb{Z}/p^{a_r}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_1}\mathbb{Z}$$

where $a_r \geq \cdots \geq a_1$ and $a_r + \cdots + a_1 = N$.

Exercise 31.3. Classify abelian groups of order 24.

Solution. We know that $A \cong H_3 \times H_2$, with $|H_3| = 3$ and $|H_2| = 2^3$. Then $H_3 \cong \mathbb{Z}/3\mathbb{Z}$, and we have

$$H_2 \cong \mathbb{Z}/8\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

each coming from the partition $3 = 3$, $3 = 2 + 1$, and $3 = 1 + 1 + 1$. □

Today we are going to prove a massive generalization. This will include the proof of the statement about finite abelian p-groups.

31.1 Classification of finitely generated modules over a principal ideal domain

Note that abelian groups are just $\mathbb{Z}$-modules, because there is a unique structure of a $\mathbb{Z}$-module on an abelian group. So I am generalizing in two ways:

- First I'm generalizing $\mathbb{Z}$ to any principal ideal domain R.
- I'm also generalizing finite to finitely generated.

Theorem 31.4. *Let R be a principal ideal domain.*[6] *Let M be a finitely generated R-module.*[7] *Then there exists an isomorphism*

$$M \cong R^{\oplus N} \oplus R/(s_1) \oplus \cdots \oplus R/(s_k)$$

where $s_i \mid s_{i+1}$ for all $1 \leq i \leq k-1$.

[6] Recall that this means that any ideal $I \subseteq R$ is generated by a single element, i.e, $I = (x)$.

[7] This means that this is generated by a finite number of elements. Equivalently, there exists a positive integer n and a surjective R-module homomorphism $R^{\oplus n} \to M$.

Let's parse this by taking $R = \mathbb{Z}$. The theorem says that any finitely generated abelian group is isomorphic to

$$\mathbb{Z}^{\oplus N} \oplus \mathbb{Z}/s_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/s_k\mathbb{Z}$$

where $N \geq 0$ and $s_i \in \mathbb{Z}$ and $s_i \mid s_{i+1}$ for all $1 \leq i < k$.

Example 31.5. If $|A| = 24$, we have $N = 0$ because A is finite. Then we need to get some sequence s_i with $s_i \mid s_{i+1}$.

A	$\mathbb{Z}/s_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/s_k\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/24\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

This is what we're doing here. We can write

$$A \cong H_{p_1} \times \cdots \times H_{p_k} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{a_{n_1}}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{b_{n_k}}\mathbb{Z}).$$

Then we can shuffle them around and see that this isomorphic to

$$(\mathbb{Z}/p_1^{\text{big}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\text{big}}\mathbb{Z}) \times (\mathbb{Z}/p_1^{\text{nextbig}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\text{nextbig}}\mathbb{Z}) \times \cdots .$$

Then the first factor is isomorphic to $\mathbb{Z}/(p_1^{\text{big}} \cdots p_k^{\text{big}})\mathbb{Z}$ and the next factor is isomorphic to $\mathbb{Z}/(p_1^{\text{nextbig}} \cdots p_k^{\text{nextbig}})\mathbb{Z}$ and so on.

Example 31.6. Let $\mathbb{K}$ be a finite field, of size q. Then the size of $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ is $q - 1$. How many abelian groups of order $q - 1$ do we know? Potentially a lot. But the interesting fact is that

$$\mathbb{K}^\times \cong \mathbb{Z}/(q-1)\mathbb{Z},$$

when the abelian group is a multiplicative group of a field. You'll prove this in a homework.

Example 31.7. Choose $A \in \mathcal{M}_{n\times n}(\mathbb{C})$. Then $\mathbb{C}^n$ is a module over $\mathbb{C}[t]$ by the multiplication

$$\mathbb{C}[t] \times \mathbb{C}^n \to \mathbb{C}^n; \quad (f(t), \vec{v}) \mapsto f(A)\vec{v}.$$

This is a module over $\mathbb{C}[t]$, and it is finitely generated. Because $\mathbb{C}[t]$ is a PID, the theorem says that

$$\mathbb{C}^N \cong \mathbb{C}[t]/(s_1) \times \cdots \times \mathbb{C}[t]/(s_k) \cong \mathbb{C}[t]/\mathfrak{p}_1^{N_1} \times \cdots \times \mathbb{C}[t]/\mathfrak{p}_\ell^{N_\ell}.$$

But over the complex numbers, the only prime ideals (except for 0) are the linear polynomials. So

$$\mathbb{C}^N \cong \mathbb{C}[t]/(x - a_1)^{N_1} \times \cdots \times \mathbb{C}[t]/(x - a_\ell)^{N_\ell}.$$

This is the Jordan normal from of A.

31.2 Proof of the classification I

Now, we're gonna prove it. Since M is finitely generated, there is a surjection

$$\phi : R^{\oplus n} \to M.$$

We can look at the kernel of this map.

Lemma 31.8. *If R is a principal ideal domain, then any submodule of $R^{\oplus n}$ is finitely generated.*

This is not obvious, but let's take this for granted for now. By the lemma, there exists a surjection

$$R^{\oplus \ell} \xrightarrow{A} \ker(\phi) \subseteq R^{\oplus m}.$$

This map A is a R-module homomorphism $R^{\oplus n} \to R^{\oplus m}$, and so can be thought of as a matrix. Also, by the first isomorphism theorem,

$$M \cong R^{\oplus m}/\ker(\phi) = R^{\oplus m}/A(R^{\oplus \ell}).$$

So to understand M, we can look at the matrix A.

Lemma 31.9. *There exist R-linear isomorphisms (these are just change of bases) $U : R^{\oplus m} \to R^{\oplus m}$ and $V : R^{\oplus \ell} \to R^{\oplus \ell}$ such that*

$$UAV = \begin{pmatrix} s_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & s_k & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Example 31.10. If $A = (p)$ is the 1×1 matrix, then $\mathbb{Z}/A(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$.

Example 31.11. If $A = \left(\begin{smallmatrix} 6 & 0 \\ 0 & 18 \end{smallmatrix}\right) : \mathbb{Z}^{\oplus 2} \to \mathbb{Z}^{\oplus 2}$, then

$$\mathbb{Z}^{\oplus 2}/A(\mathbb{Z}^{\oplus 2}) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}.$$

Lemma 31.12. *If A is a diagonal matrix, then*

$$R^{\oplus m} \cong \bigoplus_{i=1,\ldots,m} R/(a_{ii}).$$

So these three lemmas imply the classification theorem.

Proof of Lemma 31.9. The claim is that given any matrix $A = (A_{ij})$, we can change bases so that $B_{11} = \gcd(A_{ij})$. Then all other entries will be multiples of B_{11} and so we can make all other entries B_{1j} and B_{i1} to 0 by row and column operations. Do this inductively. □

32 November 27, 2017

Last time we started proving the following theorem.

Theorem 32.1. *Let R be a principal ideal domain.*[8] *Let M be a finitely generated R-module.*[9] *Then there exists an $N \geq 0$, $k \geq 0$, and $s_1, \ldots, x_k \in R$ such that*

$$M \cong R^{\oplus N} \oplus \bigoplus_{i=1}^{k} R/(s_i)$$

and $s_1 \mid s_2 \mid \cdots \mid s_{k-1} \mid s_k$. Moreover, if

$$M \cong R^{\oplus N'} \oplus \bigoplus_{i=1}^{k'} R/(s_i')$$

with $s_i' \mid s_{i+1}'$, then $N = N'$, $k = k'$, and $(s_i) = (s_i')$.

Example 32.2. Let $R = \mathbb{Z}$. Then a finitely generated $\mathbb{Z}$-module is the same thing as a finitely generated abelian group. So it is isomorphic to some

$$\mathbb{Z}^{\oplus N} \oplus \mathbb{Z}/s_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/s_k\mathbb{Z}.$$

Example 32.3. If M is an abelian group and $|M| = 49$, then M is isomorphic to one of $\mathbb{Z}/49\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

32.1 Proof of the classification II

We stated three lemmas that will help us prove the theorem.

Lemma 32.4. *Any submodule of $R^{\oplus n}$ is finitely generated.*

This allows us to find a surjection q to

$$R^{\oplus n} \xrightarrow{q} \ker(\pi) \subseteq R^{\oplus m} \xrightarrow{\pi} M.$$

Then by the first isomorphism theorem, we would have

$$M \cong R^{\oplus m}/\ker(\pi) = R^{\oplus m}/\operatorname{im}(q).$$

But our map q is $R^{\oplus n} \to R^{\oplus m}$ so it is represented by a matrix of some $m \times n$ matrix

$$A = \begin{pmatrix} a_{11} & & a_{1n} \\ & \ddots & \\ a_{m1} & & a_{mn} \end{pmatrix}.$$

So understanding M becomes understanding the image of q.

[8] This means that any ideal $I \subseteq R$ is of the form $I = (x)$.
[9] This means that there is a surjective R-module map $R^{\oplus m} \to M$.

Lemma 32.5. *There exists a basis for $R^{\oplus m}$ and $R^{\oplus n}$ such that, in this basis, A looks like*

$$A' = \begin{pmatrix} s_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & s_k & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

where $s_1 \mid s_2 \mid \cdots \mid s_{k-1} \mid s_k$.

This where we use that R is a principal ideal domain in an essential way.

Lemma 32.6. *If A can be written as A' above, then*

$$M \cong R^{\oplus N} \oplus \bigoplus_i R/(s_i)$$

where $N = m - k$.

So let us prove the lemmas.

Proof of Lemma 32.6. Note that $A' : R^{\oplus n} \to R^{\oplus m}$ is of this form. Given elements $x_1, \ldots, x_n \in R$,

$$A'(x_1, \ldots, x_n) = (f_1(x_1), \ldots, f_k(x_k), 0, \ldots, 0)$$

where $f_i : R \to R$ is given by $f_i(x) = s_i x$. Another notation for this is that

$$A' = f_1 \oplus \cdots \oplus f_n \oplus \overbrace{(0 : R \to 0) \oplus \cdots \oplus (0 : R \to 0)}^{m-k} \oplus \overbrace{(0 : 0 \to R) \oplus \cdots \oplus (0 : 0 \to R)}^{n-k}.$$

Now the claim (Claim 1 below) is that if $f_1 : X_1 \to Y_1$ and $f_2 : X_2 \to Y_2$, then

$$Y_1/f_1(X_1) \oplus Y_2/f_2(X_2) \cong (Y_1 \oplus Y_2)/(f_1 \oplus f_2)(X_1 \oplus X_2).$$

If we prove this, we are almost done because

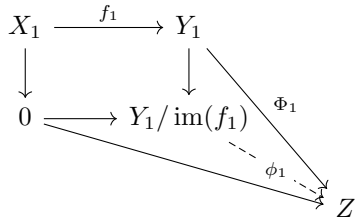
$$\begin{aligned} R^{\oplus m}/\operatorname{im}(A') &\cong R/\operatorname{im}(f_1) \oplus \cdots \oplus R/\operatorname{im}(f_1) \oplus (R/0)^{\oplus(m-k)} \oplus (0/0)^{\oplus(n-k)} \\ &\cong R^{\oplus(m-k)} \oplus R/(s_1) \oplus \cdots \oplus R/(s_k) \end{aligned}$$

But we have $M \cong R^{\oplus m}/\operatorname{im}(A)$, not $R^{\oplus m}/\operatorname{im}(A')$. Are they isomorphic? In fact, we can check that they are isomorphic (This is Claim 2). So we have

$$M \cong R^{\oplus m}/\operatorname{im}(A) \cong R^{\oplus m}/\operatorname{im}(A') \cong R^{\oplus(m-k)} \oplus R/(s_1) \oplus \cdots \oplus R/(s_k).$$

This finishes the proof of this lemma. □

Proof of Claim 1. We first look at the universal property of $Y_1/f_1(X_1)$. The universal property is that for any Z and Φ_1 satisfying $\ker(\Phi_1) \supseteq \operatorname{im}(f_1)$, there exists a unique $\phi_1 : Y_1/\operatorname{im}(f_1) \to Z$ making the following diagram commute.



The proof of this is basically the same we did for groups.

Now we are going to trace the data of the maps $Y_1/\operatorname{im}(f_1) \oplus Y_2/\operatorname{im}(f_2) \to Z$ and $(Y_1 \oplus Y_2)/\operatorname{im}(f_1 \oplus f_2) \to Z$ and then show that they contain exactly the same data. This would show that they satisfy the same universal property and thus that $Y_1/\operatorname{im}(f_1) \oplus Y_2/\operatorname{im}(f_2)$ and $(Y_1 \oplus Y_2)/\operatorname{im}(f_1 \oplus f_2)$ are isomorphic. Here is sequence of equivalences we are going to show:

(i) a map $\phi : Y_1/\operatorname{im}(f_1) \oplus Y_2/\operatorname{im}(f_2) \to Z$

(ii) maps $\phi_i : Y_i/\operatorname{im}(f_i) \to Z$

(iii) maps $\Phi_i : Y_i \to Z$ satisfying $\ker(\Phi_i) \supseteq \operatorname{im}(f_i)$

(iv) maps $\Phi : Y_1 \oplus Y_2 \to Z$ (given by $(y_1, y_2) \mapsto \Phi_1(y_1) + \Phi_2(y_2)$) satisfying $\ker(\Phi_i) \supseteq \operatorname{im}(f_i)$

(v) a map $\Phi : Y_1 \oplus Y_2 \to Z$ satisfying $\ker(\Phi) \supseteq \operatorname{im}(f_1 \oplus f_2)$

(vi) a map $\Phi : (Y_1 \oplus Y_2)/\operatorname{im}(f_1 \oplus f_2) \to Z$

First note that the data of $\phi : Y_1/\operatorname{im}(f_1) \oplus Y_2/\operatorname{im}(f_2) \to Z$ is the same as the data of two maps $\phi_i : Y_i/\operatorname{im}(f_i) \to Z$ for $i = 1, 2$. This is true in general. If we have this map ϕ, we have

$$\phi([a_1], [a_2]) = \phi(([a_1], 0) + (0, [a_2])) = \phi([a_1], 0) + \phi(0, [a_2]).$$

If we write $\phi(x, 0) = \phi_1(x)$ and $\phi(0, y) = \phi_2(y)$, then this is equal to $\phi_1([a_1]) + \phi_2([a_2])$. So they contain the same data.

By the universal property, this is equal to the data of two maps $\Phi_i : Y_i \to Z$ such that $\ker(\Phi_i) \supseteq \operatorname{im}(f_i)$. Then we can combine these two maps Φ_1, Φ_2 into a single map and say that this is the data of a map $\Phi : Y_1 \oplus Y_2 \to Z$ satisfying $\ker(\Phi_i) \supseteq \operatorname{im}(f_i)$ for each i. Here, the map Φ is defined as

$$\Phi : Y_1 \oplus Y_2 \to Z; \quad (y_1, y_2) \mapsto \Phi_1(y_1) + \Phi_2(y_2).$$

We claim that this condition $\ker(\Phi_i) \supseteq \operatorname{im}(f_i)$ can be combined into a single condition $\ker(\Phi) \supseteq \operatorname{im}(f_1 \oplus f_2)$. In other words, we are claiming that the two conditions $\ker(\Phi_i) \supseteq \operatorname{im}(f_i)$ and $\ker(\Phi) \supseteq \operatorname{im}(f_1 \oplus f_2)$ are equivalent. But

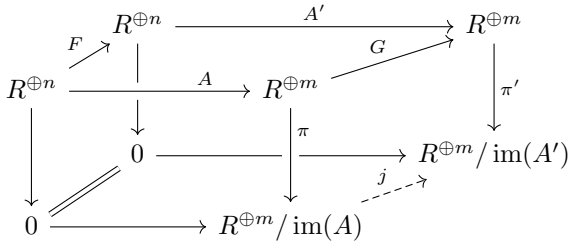
$\ker(\Phi_i) \supseteq \operatorname{im}(f_i)$ just means $\Phi_1 \circ f_1 = 0$ and $\Phi_2 \circ f_2 = 0$, and $\ker(\Phi) \supseteq \operatorname{im}(f_1 \oplus f_2)$ means $\Phi \circ (f_1 \oplus f_2) = 0$. Note that

$$(\Phi \circ (f_1 \oplus f_2))(a_1, a_2) = \Phi(f_1(a_1), f_2(a_2)) = (\Phi_1 \circ f_1)(a_1) + (\Phi_2 \circ f_2)(a_2).$$

So if we assume $\Phi \circ (f_1 \oplus f_2) = 0$ then $(\Phi_i \circ f_1)(a_1) + (\Phi_2 \circ f_2)(a_2) = 0$ for all $a_i \in X_i$ and so $\Phi_i \circ f_i = 0$. On the other hand, if we assume $\Phi_i \circ f_i = 0$ then $\Phi \circ (f_1 \oplus f_2)$ applied to anything is zero. Therefore the two conditions are equivalent.

Finally, by the universal property, $\Phi : Y_1 \oplus Y_2 \to Z$ satisfying $\ker(\Phi) \supseteq \operatorname{im}(f_1 \oplus f_2)$ has the same data as a map $\Phi : (Y_1 \oplus Y_2)/\operatorname{im}(f_1 \oplus f_2) \to Z$. This shows that the data of $Y_1/\operatorname{im}(f_1) \oplus Y_2/\operatorname{im}(f_2) \to Z$ and that of $(Y_1 \oplus Y_2)/\operatorname{im}(f_1 \oplus f_2) \to Z$ are the same. From this we conclude that $Y_1/\operatorname{im}(f_1) \oplus Y_2/\operatorname{im}(f_2)$ and $(Y_1 \oplus Y_2)/\operatorname{im}(f_1 \oplus f_2)$ are isomorphic. □

Proof of Claim 2. We want to prove that if A' is a change of basis of A, then $R^{\oplus m}/\operatorname{im}(A') \cong R^{\oplus m}/\operatorname{im}(A)$. What is a change of basis? These are basically invertible maps $F : R^{\oplus n} \to R^{\oplus n}$ and $G : R^{\oplus m} \to R^{\oplus m}$ such that $A' \circ F \cong G \circ A$. We can draw this as the top face of the following diagram.



(We don't have the map j yet.) The four faces of the cube commute, because the other three faces commute trivially. Now we want to show that there exists a unique map $j : R^{\oplus m}/\operatorname{im}(A) \to R^{\oplus m}/\operatorname{im}(A')$ that makes the entire cube commute. Here, we can use the universal property for the square on the front side. Note that $\pi' \circ G : R^{\oplus m} \to R^{\oplus m}/\operatorname{im}(A')$ satisfies

$$(\pi' \circ G) \circ A = \pi' \circ (G \circ A) = \pi' \circ (A' \circ F) = (\pi' \circ A') \circ F = 0 \circ F = 0.$$

So by the universal property, there exists a unique $j : R^{\oplus m}/\operatorname{im}(A) \to R^{\oplus m}/\operatorname{im}(A')$ that satisfies

$$j \circ \pi = \pi' \circ G.$$

This means that the right face commutes and the bottom also commutes trivially.

Because F and G are invertible, we can reverse the direction of the arrows and, by the same argument, get a map $j^{-1} : R^{\oplus m}/\operatorname{im}(A') \to R^{\oplus m}/\operatorname{im}(A)$. You can check that they are inverse, by the uniqueness of the maps, and so j is an isomorphism. Here we're not really using anything about module in particular, so this argument would work for other objects as well. □

Let us now sketch the proof of Lemma 32.5.

Proof of Lemma 32.5. Let us fix a matrix $A = (a_{ij})$. We want to show that there exists a change of basis (i.e., a sequence of invertible row and column operations) such that A becomes (in the new basis)

$$\begin{pmatrix} s_1 & \cdots & \cdots \\ \vdots & \ddots & \\ \vdots & & \ddots \end{pmatrix}$$

such that s_{11} divides any entry in its row or column. Then we can cancel out all the entries in the first row or column by adding multiples of the first row and column to other rows and columns. After this, we get

$$\begin{pmatrix} s_1 & 0 & 0 \\ 0 & \ddots & \\ 0 & & \ddots \end{pmatrix}.$$

Then we only need to deal with a smaller matrix, of size $(m-1) \times (n-1)$. We can do the same to this smaller matrix recursively. □

33 November 29, 2017

We're still proving the classification theorem for finitely generated modules over principal ideal domains.

Theorem 33.1. *Fix a principal ideal R and a finitely generated R-module M. Then*

$$M \cong R^{\oplus N} \oplus \bigoplus_{i=1}^{k} R/(s_i)$$

where $s_1 \mid s_2 \mid \cdots \mid s_k$. Moreover, k, N, and (s_i) are uniquely determined by M.

33.1 Proof of the classification III

We had three lemmas.

Lemma 33.2. *Any submodule of $R^{\oplus m}$ is finitely generated.*

This allows us to find a surjection $A : R^{\oplus n} \to \ker(\pi)$.

$$R^{\oplus n} \xrightarrow{A} \ker(\pi) \subseteq R^{\oplus m} \xrightarrow{\pi} M$$

Then the other lemmas were there to study $M \cong R^{\oplus n}/\operatorname{im}(A)$.

Lemma 33.3. *There exists a basis for $R^{\oplus n}$ and $R^{\oplus m}$ such that A is written as a diagonal matrix with diagonal entries $s_1 \mid \cdots \mid s_k$.*

Lemma 33.4. *If A is of this form, then $M \cong R^{\oplus N} \oplus \bigoplus_{i=1}^{k} R/(s_i)$.*

Sketch of proof of Lemma 33.3. Note that change of bases is a series of elementary row operations and column operations. For instance, if we a perform a column operations of adding a times the ith column to the jth column, this is like

$$A_1 = \begin{pmatrix} & | & & | & \\ \cdots & v_i & \cdots & v_j & \cdots \\ & | & & | & \end{pmatrix} \mapsto \begin{pmatrix} & | & & | & \\ \cdots & v_i & \cdots & av_i + v_j & \cdots \\ & | & & | & \end{pmatrix} = A \begin{pmatrix} 1 & & & \\ & \ddots & a & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

Now the claim is that there exist bases in which A becomes something like

$$A_1 = \begin{pmatrix} s_1 & \cdots & \cdots \\ \vdots & \ddots & \\ \vdots & & \ddots \end{pmatrix}$$

where s_1 divides all the other entries of A_1. Given this claim, all the entries in either the first row or the first column can be written as $a_{ij} = s_1 b_{ij}$. So we

can use elementary column operations to make all the first row elements (other than s_1) zero,

$$\begin{pmatrix} s_1 & 0 & 0 \\ \vdots & \ddots & \\ \vdots & & \ddots \end{pmatrix}$$

and then use elementary row operations to make make the first column (except for s_1) zero,

$$\begin{pmatrix} s_1 & 0 & 0 \\ 0 & \ddots & \\ 0 & & \ddots \end{pmatrix}.$$

Now let me give a sketch of the claim. It actually suffices to show that for a 2×1 column matrix $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ so that

$$A \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \gcd(a,b) \\ \bullet \end{pmatrix}.$$

The reason is that we can use this 2×2 matrix to make a gcd of more and more entries, so that a_{11} becomes the gcd of the all the entries.

So how do we prove it for 2×1 matrices? We know that there exist $u, v \in R$ such that $au + bv = g = \gcd(a,b)$, where $(g) = (a,b)$ by definition. Then we can put

$$A = \begin{pmatrix} u & v \\ \bullet & \bullet \end{pmatrix}.$$

But we have to find the other entries, and we don't really care about what exactly these are. The only condition that needs to be met is that the determinant is 1 so that the matrix is invertible. But because $au + bv = g$ is the gcd, it turns out that $\gcd(u,v) = 1$. So there are w, x such that $xu - wv = 1$. Then we can set $A = \left(\begin{smallmatrix} u & v \\ w & x \end{smallmatrix}\right)$. □

For Lemma 33.2, just Google "Noetherian ring". It can be shown that any principal ideal domain is Noetherian. Also, if R is Noetherian and M is a finitely generated R-module, then every submodule of M is finitely generated.

33.2 Towards a classification of finite groups

Let us move to a new topic. In this class we proved classification theorems of

- finitely generated abelian groups (and so finite abelian groups),
- finitely generated R-modules (for R a principal ideal domain).

But we started this class with groups. Can we classify finite groups? In other words, is there some "list" of groups we can write so that all finite groups are "built out" of these groups on the list? We can start classifying groups by its order. (I'm writing $\mathbb{Z}/n\mathbb{Z}$ as C_n.)

$\lvert G\rvert$	G
1	$\{e\}$
2	C_2
p	C_p
p^2	C_{p^2}, $C_p \oplus C_p$
pq	C_{pq} or $\mathbb{A}_{pq}$
8	C_8, $C_2 \oplus C_4$, $C_2 \oplus C_2 \oplus C_2$, Q_8, D_8

Table 5: List of groups of a certain order

We have proved that every groups of order p^2 are either C_{p^2} or $C_p \oplus C_p$. Then in the homework due today, you proved that every group of order pq is either C_{pq} or $\mathbb{A}_{pq} = \{\text{affine } \mathbb{F}_p \to \mathbb{F}_p \text{ of order } q\}$. The two groups Q_8 and D_8 are not isomorphic, because Q_8 have 2 elements of order 2 where D_8 have 5 elements of order 2. Is there no other group of order 8? I think these are all, but it is not at all clear that our list is exhaustive.

This seems like not a very easy task. We need a systematic way of organizing groups, and something like prime factorization seems reasonable, because we know how to classify groups whose order has a simple prime factorization.

If we can find a normal subgroup $H \lhd G$ with $H \neq \{e\}, G$, we can take the quotient G/H. Here, H and G/H have order dividing $|G|$. So maybe we can understand G by understanding H and G/H. Because H is normal, there is a conjugation action

$$G \to \mathrm{Aut}(H); \quad g \mapsto (h \mapsto ghg^{-1}).$$

But note that inner automorphisms $\mathrm{Inn}(H)$ of H is a normal subgroup of $\mathrm{Aut}(H)$. So we can take the quotient

$$\mathrm{Out}(H) = \mathrm{Aut}(H)/\mathrm{Inn}(H).$$

So we can project down to

$$G \to \mathrm{Aut}(H) \to \mathrm{Out}(H)$$

and its composition $H \hookrightarrow G \to \mathrm{Out}(H)$ is trivial. So by the universal property, we would get

$$G/H \to \mathrm{Out}(H).$$

Proposition 33.5. *There are concrete ways to construct G by understanding group homomorphism $G/H \to \mathrm{Out}(H)$.*

But there is a fatal flaw in this plan. What if G has no nontrivial normal subgroups. So we need to understand these groups.

34 December 1, 2017

Last time we talked about classifying finite groups. Our goal was to make a list of "basic" groups out of which all finite groups are "built". Here was the strategy. Assume that we completely understand all groups of order smaller than $|G|$. First, find a $H \lhd G$ such that $H \neq \{e\}, G$. Then we can take the quotient group

$$H \hookrightarrow G \to G/H.$$

Then the claim I made is that the group homomorphism

$$G/H \to \mathrm{Out}(H)$$

essentially tells us about G. I'm not going to prove this but it is not obvious. But there was a fatal flaw in this plan. What if there are no normal subgroups $H \lhd G$ such that H is neither $\{e\}$ nor G?

34.1 Introduction to simple groups

Definition 34.1. A group G is **simple** if $H \lhd G$ implies $H = \{e\}$ or $H = G$.

Example 34.2. $G = \{e\}$ is simple, and also $G = \mathbb{Z}/p\mathbb{Z}$ for p prime are simple. Also, $A_5 = \ker(S_5 \to \mathbb{Z}/2\mathbb{Z})$ is simple. Also, $A_n = \ker(S_n \to \mathbb{Z}/2\mathbb{Z})$ is simple if $n \neq 4$.

Theorem 34.3 (or cultural belief)**.** *We have "classified" all finite simple groups.*

By this, I mean that there is a reasonable and exhaustive list (although infinite) of all simple groups, with a somewhat concrete description. The completion of the proof was announced at 2004, and then in 2008 somebody found a mistake in the computation of the character table. Then it was revised. Mathematicians aren't robots, and they can make mistakes if the proof is something like 2000 pages. But I want to give you the impression that modern mathematics is not really set.

Theorem 34.4 (Feit–Thompson)**.** *If G is finite and simple, and G is not cyclic, then $|G|$ is even.*

This should be very non-obvious for you. This theorem got Thompson a Fields medal.

Let G be finite and simple. Then we can look at the maximal normal subgroup H of G that is not G. Then G/H is going to be simple. The reason is that if G/H has a nontrivial normal subgroup, the inverse image under $G \to G/H$ is going to be a bigger normal subgroup. So we have G/H is simple. We can do the same thing for H and then do this repeated to get a sequence $\{e\} \lhd H_k \lhd \cdots \lhd H_1 \lhd G$.

$$\begin{array}{ccccccccccc}
\{e\} & \hookrightarrow & H_k & \hookrightarrow & H_{k-1} & \hookrightarrow & \cdots & \hookrightarrow & H_1 & \hookrightarrow & G \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow \\
 & & H_k & & H_{k-1}/H_k & & \cdots & & H_1/H_2 & & G/H_1
\end{array}$$

Here, the successive quotients H_i/H_{i+1} are simple and called the **composition factors** of G.

Theorem 34.5 (Jordan–Hölder)**.** *The list $\{H_i/H_{i+1}\}$ is independent of the choices of H_i.*

But the list does not uniquely determine the group G.

Example 34.6. Let $G = C_4$ and $H = \{0, 2\}$. Then $G \ncong H \times G/H$. Likewise, for $G = S_3$ and $H = C_3$, we have

$$C_3 \hookrightarrow S_3 \longrightarrow C_2.$$

Here there exist an injection $G/H \hookrightarrow G$ such that $G/H \hookrightarrow G \to G/H$ is the identity map. Then we say that this is a split exact sequence. This is called a **semi-direct product**.

Definition 34.7. We say that G is an **extension** of B by A if $A \lhd G$ and $B \cong G/A$.

34.2 What next?

So what did we do in this class? We have seen some words like groups, rings, modules. But there is supposed to be some motivation. The concept of groups, rings, and other objects are supposed to reflect the history of how numbers were developed.

Let me give a recreation of history. When you were like four years old, you were taught numbers $0, 1, 2, \ldots$. At this point, you probably did not know that you could add numbers. But as the concept of taking unions came about, you might of learned how to add. Then you might have at some point told that you could also multiply numbers. Addition is not invertible and somebody might have wanted to make addition invertible in numbers. This led to the notion of the ring of integers $\mathbb{Z}$. Then if you want multiplication also to be invertible, you would get its field of fractions $\mathbb{Q}$.

But there is also the real numbers $\mathbb{R}$. How do you construct real numbers? Not all real numbers are solutions of rational coefficient polynomials. So you need some kind of limit to construct $\mathbb{R}$, or $\mathbb{C}$. Analysis deals with limits, and you could take courses like Math 112 or 113.

For the geometric side, there are Lie groups, like $S^3 \subseteq \mathbb{R}^3$ we have seen in the optional problems. There is a course on Lie groups and algebras, Math 222. Algebraically, algebraic geometry deals with spaces that look like zero sets of polynomials. For instance, spaces are $\{(x, y) \in \mathbb{R}^2 : y - x^2\} = 0$. This will look like a parabola inside $\mathbb{R}^2$. Algebraic geometers call these spaces schemes. There are weird schemes, like $k[\epsilon]/(\epsilon^2)$, which might not match with your notion of spaces. There are courses like Math 233a that teach you about schemes.

You could also go and study number theory. There are really interesting problems, like studying primes in $\mathbb{Z}[i]$. For instance, what is a prime $p \in \mathbb{Z}$ that is a norm of something in $\mathbb{Z}[i]$. There are many number theory courses, and

you could also go and study elliptic curves. These curves are also schemes, but number theorists use them to study numbers.

Topology studies spaces, but there are shapes that we can't draw to study. So people have developed ways of getting a group or a ring from a space X. For any space X, $\pi_1 X$ is a group, $H_* X$ and $\pi_{\geq 2} X$ are abelian groups, and $H^* X$ is a ring. Math 131 and 132 will deal with these.

Index