MATH 120 - Groups and Rings

Instructor: Church; Notes: Adithya Ganesh

June 13, 2018

Contents

1 Lecture 4:

1.1 Homomorphisms

Two ways in which a homomorphisms can arise.

- Define a function completely, and ask if its a homomorphism.
-

Example. Consider the group $GL_2\mathbb{R}$. Consider the function called the determinant:

$$\det GL_2\mathbb{R} \to \mathbb{R}^x.$$

Fix matrix

$$\det \begin{pmatrix} a & b \\ cd & \end{pmatrix} = ad - bc.$$

We know the value of the function unambiguously. The way to determine whether this is a homomorphism is to ask whether

$$\det(AB) = \det A \det B.$$

Side comment on notation. Note that $\mathbb{R}^x$ should be viewed as the nonzero elements of $\mathbb{R}$ as a group under multiplication.

$$\mathbb{R}^x = \mathbb{R} - \{0\}, \times$$
$$\mathbb{C}^x = \mathbb{C} - \{0\}, \times.$$

What about $\mathbb{Z}^x$? Clearly the nonzero elements of $\mathbb{Z}$ under multiplication is not a group.

So concretely,

$$\mathbb{R}^x = \{\text{elements of } \mathbb{R} \text{ with multiplicative inverses in } \mathbb{R}\}$$

Generalizing this to $\mathbb{Z}^x$, we know $\mathbb{Z}^x = \{1, -1\}$ all have inverses.

Another example:

$$(\mathbb{Z}/8\mathbb{Z})^x = \{1, 3, 5, 7\}$$

In general,

$$(\mathbb{Z}/n\mathbb{Z})^x = \{m \text{ such that } n \text{ and } m \text{ are relatively prime}\}$$

Example. Consider the absolute value function:

$$\begin{aligned} \mathbb{R}^x &\to \mathbb{R}^x_{>0} \\ x &\mapsto |x|. \end{aligned}$$

Since it is true that

$$|xy| = |x||y|,$$

we know that the absolute value is a homomorphism.

Example. Consider the sign function.

$$\begin{aligned} \mathbb{R}^x &\to \{\pm 1\} \\ x &\mapsto \begin{cases} +1; & \text{if } x > 0 \\ -1; & \text{if } x < 0. \end{cases} \end{aligned}$$

Clearly,

$$\operatorname{sign}(xy) = \operatorname{sign}(x)\operatorname{sign}(y).$$

Example. Consider the map

$$\begin{aligned} \mathbb{R} &\to \mathrm{GL}_2\,\mathbb{R} \\ x &\mapsto \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix} \end{aligned}$$

Is it true that

$$(cos(x+y), -\sin(x+y), sin(x+y), cos(x+y)) = (cosx - sinxsinxcosx)(cosy, -siny, siny, cosy)$$

$$\begin{pmatrix} \cos x + y & -\sin(x+y) \\ \sin(x+y) & \cos(x+y) \end{pmatrix} = \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix} \begin{pmatrix} \cos y & -\sin y \\ \sin y & \cos y \end{pmatrix}$$

This is tricky, but it is

$$\text{rot}(x+y) = rot(x) \circ \text{rot}(y)$$

Notice that we can also show that there is a homomorphism on rotation without knoing the exact formula for the matrix.

1.2 Approach 2: Bottom-up homomorphisms

In this setting, partially define the map. Define the function on generators for a group. Then, ask if there exists a homomorphism (alternative phrasing: ask if it extends to a homomorphism).

Example. Let $G = \mathbb{Z}_4 = \{1, x, x^2, x^3\}$ with $x^4 = 1$.

Questions we can ask

Is there a homomorphism from $f_1 : \mathbb{Z}_4 \to GL_2\mathbb{R}$ with $f(x) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$?

Is there a homomorphism with $f_2(x) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$, and $f_3(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Clearly f_1 and f_3 with matrix multiplication operations end up being homomorphisms (since the matrix raised to fourth powers are the identity). But f_2 is not: since if you raise it to the fourth power, you do not get the identity.

Key observation:

- Whether or not there is a homomorphism, there is at most one. i.e. If there is one, it's unique. Why? Because if it is a homomorphism, we must have

$$f_1(x) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

$$f_1(x^2) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2.$$

$$\cdots$$

  We also know that

$$f_1(x^4) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4$$

  and

$$f_1(x^5) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^5$$

  But $x = x^5$, so $f(x)$ must equal $f(x^5)$!

  But the element C from f_3 has order 2! We must have $C^4 = 1$ to obtain a well defined homomorphism, and this is fine).

  There is only one homomorphism for *each question* above.

Question: is there a homomorphism $f : \mathbb{Z} \to \{\pm 1\}$ with $f(2) = 1$?

Clearly, there is a trivial homomorphism $f(anything) = 1$. We also have $f'(k) = (-1)^k$.

If G is generated by $\{x, y, z\}$ and you pick $p, q, r \in H$, there's at most one homomorphism.

Suppose you know $f_1 : G \to H$ and $f_2 : G \to H$. You want to know if $f_1 = f_2$. Just need to check if $f_1(x) = f_2(x)$ for all x.

This is very much like the theorem in linear algebra that says the value of a linear transformation is determined by its value on a basis.

Key observation 2. In general, its hard to know if there is a homomorphism or not. Suppose we had asked, instead that

Example. Let $G =$ subgroup of $GL_2\mathbb{C}$ generated by $a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Is there a homomorphism from $G \to \{\pm 1\}$ with $f(a) = -1$ and $(b) = -1$?

Problem: we don't have a list of all the coincidences in the group G. For example, suppose we had to know $a^2bab = -1$ and $b^{-1}aba^2b = 1$. Without the list of coincidences, can't check whether this extends to a valid homomorphism.

In the previou ssetting, we really do have a list of complete concidences, $x^k = x^l$, only if $k \equiv l \pmod 4$.

In the future, we will use the following notation, $Z_4 =< x|x^4 = 1 >$ which is called a group presentation. The only relation you need to know and all other relations follow from that.

Q: With enough computation, is it possible to systematically enumerate these coincidences?

A: For this subgroup of GL2 C, the answer is yes (since there are only 8 elements). But for an infinite group, this isn't in general possible, because you run into the halting problem. This is broadly referred to as the "word problem".

Frequent setting: you can have homomorphisms f with $f : G \to (X)$ in a set, $Perm(X) =$ group of permutations (bijections) with $g : X \to X$.

2 Lecture 5

Notation: given a subset $T \subset G$, the notation

$$< T >= \text{subgroup of } G \text{ generated by } T$$

$$< T >= \cap H_{\text{all subgroups } H < G}$$

Recall:

$$\text{Perm}(X) = \text{group of bijections } g : X \to X \text{ under O}$$

The symmetric group S_n is defined as

$$S_n = \text{Perm}(\{1, 2, \ldots, n\})$$

Note the idea of cycle decomposition. Suppose we have a setting where

$$\begin{aligned} g(1) &= 4 \\ g(2) &= 3 \\ g(3) &= 2 \\ g(4) &= 5 \\ g(5) &= 1 \end{aligned}$$

We can also draw out a diagram.

Alternatively, we can decompose this into cycles. Can write this as

$$g = (1\ 4\ 5)(2\ 3)$$

This is called the "cycle decomposition" of g, where we express the group element as a product of disjoint cycles.

Usually we drop length-1 cycles. For example, in a setting with

$$h = (1\ 2)(3)(4)(5),$$

we would usually write

$$h = (1\ 2)$$

Note that symmetric groups are not abelian! The order of function composition definitely matters. However - disjoint cycles do commute with each other.

What is the order of a permutation $\sigma \in S_n$?

For example, the order of $\sigma = (2\ 3)$ is two. In general, the order of a cycle decomposed permutation is the LCM of the cycle lengths.

Cycle decomposition is unique up to ordering of each cycle + ordering withing each cycle.

2.1 Order

HW question. Recall the optional homework question - had to show that if $|g| = 2$, then $|G|$ is even.

More general statement. More generally, if $|g| = k$, then $|G| \equiv 0 \pmod{k}$. (If g is a generator of the group G, then we know that $|G| = k$ exactly).

Remark. Any element g corresponds to a cyclic subgroup $< g >$.

Even more general. (Lagrange's Theorem) If H is any subgroup of G, then $|G|$ is divisible by $|H|$.

Notation. The index of H in G is the whole number $|G|/|H|$. So, for example, if $|G| = 100$, and $H < G$, with $|H| = 25$, then the index $[G \cdot H] = 4$.

Importantly, this makes sense even when we have infinite groups. Consider $G = \mathbb{Z}$, with $H < G =$ the multiples of 2. We can still say that $[G \cdot H] = 2$.

Example. *Let p be a prime number. Suppose $|G| = p$. Then every $g \in G$ has $|g| = 1$ or $|g| = 7$. This means that $G \equiv \mathbb{Z}_7$.*

Outline of proof. Define the following equivalence relation. Given a subgroup $H < G$, we say $x \sim y$ iff there exists $h \in H$ such that $y = xh$.

This is an equivalence relation exactly because H is a subgroup. Note that:

- Reflexivity holds. (since $1 \in H$)
- Symmetry holds. (since H is closed under inverses)
- Transitivity holds. (since H is closed under multiplication)

We will say that the equivalence class of x is called xH is called its left coset (of H in G). In particular,

$$\begin{aligned} xH &= \{y | x \sim y\} \\ &= \{y | \exists h \text{ s.t. } y = xh\} \\ &= \{xh | h \in H\} \end{aligned}$$

The key to the argument, which we will show on Friday, is that $|xH| = |H|$. Therefore, G can be partitioned into a bunch of cosets (which are all the same size); and hence

$$|G| = (\#\text{ of cosets}) \cdot |H|$$

3 Lecture 6

Problem setting. Let G be a group, $H < G$, and let $g \in G$. We will discuss three notions of translations of H by g.

- *Left coset.* $\{gH = \{gh | h \in H\}\}$
- *Right coset.* $\{Hg = \{hg | h \in H\}\}$
- *Conjugate (of H by g)* $gHg^{-1} = \{ghg^{-1} | h \in H\}$

Example. *Let $G = S_5$, and suppose $H = \{\sigma \in G | \sigma(2) = 2\}$. Let $g = (123)(45)$. Want to find gH, Hg, and gHg^{-1}.*

Note that $|G| = 120$, $H = 24$. Note that $|gH| = |Hg| = |gHg^{-1}| = 24$. Compute the cosets and the conjugate.

Note that

$$gH = \{\sigma \in S_5 | \sigma(2) = 3\}.$$
$$Hg = \{\sigma \in S_5 | \sigma(1) = 2\}.$$
$$gHg^{-1} = \{\sigma \in S_5 | \sigma(3) = 3\}.$$

Also, it is clear that gH and Hg are not subgroups (not preserved under composition). However, gHg^{-1} is a subgroup.

Example. *Let $G = Isometries(\mathbb{R}^2)$, that is, distance preserving bijections in the plane. Let*

$$H = \{h \in G | h(\mathbf{0}) = \mathbf{0}\}$$
$$g = 90^\circ \text{ rotation around } (1, 0)$$

Compute the cosets and conjugate.

We can compute that

$$gH = \{\gamma \in G | \gamma(\mathbf{0}) = g(\mathbf{0})\}$$
$$Hg = \{\gamma \in G | \gamma(q) = \mathbf{0}\}$$
$$gHg^{-1} = \{\gamma \in G | \gamma(p) = p\}$$

(where $p = g(\mathbf{0})$).

Question 1 on HW2. Answer is $K = \mathbb{Z}$. Look at solutions for details.

On homework, discussed the notion of a kernel. If $f : G \to Q$, then

$$\mathrm{Ker}(f) = \{g \in G | f(g) = 1\}.$$

We can ask a question. Can every subgroup $H < G$ be the kernel of something?

Consider an example of $G = S_3 = \{e, (12), (23), (13), (123), (132)\}$. Set $H = \{e, (12)\}$.

Question. If I tell you I have a homomorphism $f : G \to Q$, with $\mathrm{Ker}(f) = H$, how can you prove I'm lying?

Answer. Write out where each element maps to:

$$\begin{aligned} e &\to e \\ (12) &\to 1 \\ (23) &\to a \\ (13) &\to b \\ (123) &\to c \\ (132) &\to c^{-1} \end{aligned}$$

Note that

$$(12)(23) = (123)$$

so

$$f(12)f(23) = f(123).$$

Hence $1a = c$, that is $a = c$. Similarly, $(13)(12) = (123)$ implies $b = c$. Finally, $(23)(13) = (123)$ implies $ab = c$. This implies $a \cdot a = a$, which gives $a = 1$.

That means, H was not the kernel. That means, the kernel was the entire group.
Proposition. *If $H < \mathrm{Ker}(F)$, then $gHg^{-1} < \mathrm{Ker}(f)$ also, for all $g \in G$.*

Proof. Note that

$$\begin{aligned} f(ghg^{-1}) &= f(g)f(h)f(g)^{-1} \\ &= f(g)1f(g)^{-1} = 1. \end{aligned}$$

Therefore, this shows that if $K = \mathrm{Ker}(f)$, we must have $gKg^{-1} = K$ for all $g \in G$. □

Definition. *We say that a subgroup $K < G$ is normal if $gKg^{-1} = K$ for all G. Notation: we write $K \triangleleft G$.*

Note that the kernel of any homomorphism is always a normal subgroup.

This is completely unlike linear algebra. You need a normal subgroup to be the kernel of something.

For normal subgroups, left cosets equal right cosets, since $gKg^{-1} = K$ implies $gK = Kg$. This is not true otherwise.

4 Lecture 7

Recall the definition of a normal subgroup.

Definition. *A subgroup $N < G$ is normal if $gN = Ng$ for all $g \in G$.*

(Obviously, if G is abelian, then every subgroup of G is normal.)

Recall, that the coset gN is the equivalence class of g under the equivalence relation $G \sim h$ if $h = gn$ for some $n \in N$.

Last week, we saw that if you have some homomorphism $f : G \to H$, then $\mathrm{Ker}(f)$ is always a normal subgroup of G.

Question. Give a normal subgroup $N \triangleleft G$, can we find a group Q and a homomorphism $f : G \to Q$, with $\mathrm{Ker}(f) = N$?

Example. *Take $G = \mathbb{Z}$, and let $N = 2\mathbb{Z}$. Does there exist some $f : \mathbb{Z} \to Q$ with $\mathrm{Ker}(f) = 2\mathbb{Z}$?*

Let's first establish what this means:

$$f(n) = 1 \text{ if } n \text{ even}$$

$$f(n) \neq 1 \text{ if } n \text{ odd}$$

Now, from Friday, call $f(1) = q$. Then we know that $f(n) = q^n$. We must have

$$f(-1) = q^{-1} = q \neq 1$$

$$f(0) = q^0 = 1$$
$$f(1) = q \neq 1$$
$$f(2) = q^2 = 1$$
$$f(3) = q^3 = q \neq 1.$$

Therefore, the only possible group has two elements, 1 and q (with $q^2 = 1$).

Example. *Let $G = \mathbb{Z}$, and $N = 10\mathbb{Z}$. We would like some map $f : \mathbb{Z} \to Q$, with $\mathrm{Ker}(f) = 10\mathbb{Z}$.*

We know that all of the multiples of 10 must map to the identity in Q. But we know more, we can state that

$$f(m) = f(n) \Leftrightarrow 10|(n - m).$$

The $\Leftarrow$ direction is easy. The $\Rightarrow$ direction is true because if not, the kernel would be bigger.

Note that

$$A = \{\ldots, -10, 0, 10, 20\} \text{ map to 1 in } Q$$
$$B = \{\ldots, -9, 1, 11, 22\} \text{ map to other element in } Q$$
$$\ldots$$
$$J = \{\ldots, -1, 9, 19, 29\} \text{ map to a tenth element in } Q.$$

Insight: what if we call $Q = \{A, B, C, \ldots, J\}$. Define the group operation $B + C = D$, and we can take any element from these subsets, and get the "answer" D.

So $Q = \mathbb{Z}/10\mathbb{Z}$, which is our quotient group. In other words:

$$10\mathbb{Z} = \mathrm{Ker}(\mathbb{Z} \twoheadrightarrow \mathbb{Z}/10\mathbb{Z}).$$

or:

$$N = \mathrm{Ker}(G \twoheadrightarrow G/N).$$

Aside on notation: [1]

We now formally define quotient groups.

Definition. *Given a group G and a normal subgroup $N \triangleleft G$, the quotient group G/N is defined by:*

- *its elements are the cosets gN (note that left = right cosets for a normal subgroup). In other words, these are equivalence classes $\overline{g}$ under the notation $g \sim h$ iff $h = gn$.*[2]
- *Its group operation is $\overline{g} \cdot \overline{h} = \overline{gh}$.* **We need to check that this is well defined! This is critical, and this is where it matters that N is normal.**

Check that the quotient group is a group.

- Identity: $\overline{1} \cdot \overline{h} = \overline{1h} = \overline{h} = \overline{h \cdot 1} = \overline{h} \cdot \overline{1}$
- Associativity: $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

Several comments: [3] [4]

Note that there is a canonical surjective homomorphism

$$\pi : G \twoheadrightarrow G/N$$

that takes $g \mapsto \pi(g) = \overline{g}$.

Remark. *What is the size of the quotient group? Note that*

$$|G/N| = \text{ of cosets of } N \text{ in } G$$

$$= \textit{index}[G : N]$$

If $|G|$ is finite, then

$$|G/N| = |G|/|N|$$

Now, we can still define the index of two groups that are infinite. Easy example:

$$[\mathbb{Z} : 10\mathbb{Z}] = |\mathbb{Z}/10\mathbb{Z}| = 10.$$

$$|\mathbb{Z}|/|10\mathbb{Z}| = \infty/\infty.$$

[1] Note that $\twoheadrightarrow$ indicates a surjective map, and $\hookrightarrow$ indicates an injective map.

[2] On equivalence classes: $g \sim h \Leftrightarrow h \in \overline{g} \Leftrightarrow \overline{g} = \overline{h}$

[3] This is somehow similar to compiled languages. Check once that the quotient group is well defined, and know that can write "loose" notation that can't go wrong.

[4] (Note that 3.1 in the book is pretty confusing)

Theorem. *(First isomorphism theorem.) If $f : G \to H$ is any homomorphism, then*

$$G/\operatorname{Ker}(f) \cong \mathit{Im}(f).$$

To name the map:

$$\psi(\overline{g}) = f(g).$$

This theorem seems really simple - but its subtle, because its not super clear if its obvious or if we need to prove it.

Checking that $\overline{g} \cdot \overline{h} = \overline{gh}$ is well defined. Suppose that $\overline{g} = \overline{a}$ and $\overline{h} = \overline{b}$. Then

- $\overline{g} \cdot \overline{h} = \overline{gh}$
- $\overline{g} \cdot \overline{b} = \overline{gb}$
- $\overline{a} \cdot \overline{b} = \overline{ab}$

We need to check that

$$\overline{gh} = \overline{gb} = \overline{ab}.$$

Suppose $\overline{h} = \overline{b}$. Then there exists $m \in N$ such that $b = hm$. We have

$$(gb) = (gb)m,$$

so $\sim gh$, i.e. $\overline{gb} = \overline{gh}$.

Note that $\overline{a} = \overline{g}$, i.e. there exists $n \in N$ such that $a = gn$. Therefore -

$$ab = gnb = gbn'.$$

Therefore $ab \sim gb$ so $\overline{ab} = \overline{gb}$.

For the above, we have used normality, since we know that $nb \in Nb = bN$.

5 Lecture 8

5.1 More on conjugation

Comment from office hours. It was brought up that we don't really have that many examples of abelian groups. D_{2n} is generally non-abelian (D_2 is the only abelian case).

One of the main topics today will be *conjugation.* Earlier, we saw that gNg^{-1} is a notion of "translation" by N. More explicitly, let us analyze a vs gag^{-1}.

Where might you have seen an equation like $b = gag^{-1}$? One place is linear algebra — if A and B are matrices that represent the same linear transformation, but in different bases, then you get

$B = CAC^{-1}$ where C is the change of basis matrix. In this setting A and B are "the same," but in different coordinate systems.

Suppose we have two sets $\{x, y, z, w\}$ and $\{1, 2, 3, 4\}$ with the bijection f where $x \mapsto 1$, $y \mapsto 2$, $z \mapsto 4$, $w \mapsto 3$. Suppose we had a permutation $\sigma \in \text{Perm}(\{x, y, z, w\})$ where

$$\sigma = (xyz)(w).$$

The claim: the earlier bijection lets us "turn" this into a bijection of the set $\{1, 2, 3, 4\}$. We can remap the permutations to obtain

$$1 \to x \to y \to 2$$
$$2 \to y \to z \to 4$$
$$3 \to w \to w \to 3$$
$$4 \to z \to x \to 1.$$

This composition can be expressed as $f\sigma f^{-1}$.

More commonly, suppose we have some $g \in S_n$, and some $\sigma \in S_n$. We can consider a conjugation $g\sigma g^{-1}$.

Example. *Let σ = (1 2 7)(5 8)(3 4), and let $g(i) = i + 10 \pmod{100}$. Then*

$$g\sigma g^{-1} = \textit{(11 12 17)(15 18)(13 14).}$$

Definition. *Let G be a group and let $a, b \in G$. We say that a, b are conjugates (in G) if there exists $g \in G$, such that*

$$b = gag^{-1}$$

Notes:

- *This is an equivalence relation.*
- *The equivalence classes are called conjugacy classes.*
- *Intuitively, the conjugacy classes group elements with the "same structure."*
- *If G is abelian, then conjugacy classes are just $\{1\}, \{a\}, \{b\}, \ldots$.*

Question. When are two permutations $\sigma, \tau \in S_n$ conjugates?

Any permutation with a cycle decomposition in a "3-2-2" pattern is conjugate to σ = (1 2 7)(5 8)(3 4), for example (14 3 2)(7 8)(10 11).

Answer. If their cycle decompositions have the same number of cycles of each length.

Proposition. *Every $A \in GL_2\mathbb{C}$ is conjugate to some B of the form $B = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$.*

If you apply this B to $e_1 = [1\ 0]$, you get $Be_1 = xe_1$, i.e. e_1 is an eigenvector. So this holds because every A has an eigenvector.

Note. Fix some element $g \in G$. Consider the function $\alpha_g : G \to G$ given by conjugation: $\alpha_g(h) = ghg^{-1}$. Is this a homomorphism?

Consider

$$\alpha_g(hk) = ghkg^{-1}$$
$$\alpha_g(h)\alpha_g(k) = ghg^{-1}gkg^{-1} = ghkg^{-1}.$$

So yes, it is a homomorphism. What is the kernel of this function? Just the identity.

If $f : G \to H$ is a homomorphism, then the following are equivalent:

- f is injective
- $\mathrm{Ker}(f) = \{1\}$.

This implies that α_g is actually an isomorphism from G to itself.

Question. Do the size of conjugacy classes divide the order of the group? A: Yes, but not for the same reason as in Lagrange's theorem.

5.2 Group actions

We start with the definition.

Definition. *An action of a group G on a set X is a homomorphism $\alpha : G \to Perm(X)$.*

In other words, to each $g \in G$, we can associate a function $\alpha_g : X \to X$ such that

$$\alpha_g \circ \alpha_h = \alpha_{gh}.$$

This is almost the same is a group of functions, but the only difference is that nobody says that this homomorphism has to be injective.

Note: this is discussed in section 1.7 in the text, but it uses a different framework.

Concretely, suppose we have a group D_8, with a map to Perm$(\mathbb{R}^2)$. Since for example "rotation by 90 degrees" can be viewed as a translation in the plane. So — this is an action of D_8 on $\mathbb{R}^2$.

The *action* is a realization of the group as functions on the plane. The important thing here is *how the homomorphism is defined* (not the given D_8 or $\mathbb{R}^2$).

But note that group actions don't always have natural geometric interpretations.
Example. *Let $G = \mathbb{Z}/7\mathbb{Z}$, and let $X = \{1, 2, 3, 4\}$. Claim: any action of G on X is trivial.*

Notation in book. Suppose we have $x \in X$, and we can consider $\alpha_g : X \to X$. Then we can view $\alpha_g(x) \in X$. One thing the book points out is that you can write $\alpha_g(x)$ as $g \cdot x$. But the $\alpha_g(x)$ notation is arguably a bit clearer.

6 Lecture 9

We start be defining the notion of a *product group.* If A and B are groups, then we can define a group on

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

The operation is defined component wise:

$$(a, b) \cdot (\alpha, \beta) = (a\alpha, b\beta).$$

Comments on question 6. Can we find some group K such that $n(K, G) = |G|^2$. As many reasoned correctly, we must have K have two generators. The reason $\mathbb{Z}^2$ does not work is because although it is generated by two elements $(1, 0)$ and $(0, 1)$, this group is abelian. Now, the number of homomorphisms $n(\mathbb{Z}^2, G)$, is

$$n(\mathbb{Z}^2, G) = |\{(g, h) | g \in G, h \in G, gh = hg\}| \leq |G|^2.$$

(Mentioning $\mathbb{Z}^2$ and arguing why it is wrong is much better than turning in a "false" proof that $\mathbb{Z}^2$ works.)

Now, we want to build some $K = F_2$, defined as the "free group on two generators." (Free, here is a semi-technical term, see the idea of a "free module.") We want:

- F_2 is generated by two elements.
- a and b don't satisfy any relations except those that are forced by the group axioms.

Now, how do we turn this vague desire into an actual group? The challenge, as it turns out, is mainly in establishing associativity.

Let $F_2 = \langle a, b \rangle$; this is what we hope to be able to write.

- First try, let F_2 be the set of finite strings on the alphabet $\left\{a, b, \overline{a}, \overline{b}\right\}$, with the operation = concatenation. (Similar to Kleene closure.) Problem: there is no inverses, since $(ab)BA = abBA$.
- Second possibility: define an equivalence relation on $\{a, b, A, B\}^*$, where $waAu \sim wu$, $wAau \sim wu$, $wbBu \sim wu$, $wBbu \sim wu$, and if $w \sim w'$ and $u \sim u'$, then $wu \sim w'u'$.

  Possible problem. How to show that we haven't identified too many things together?
- Third possibility: define a string to be "reduced" if it has no aA, Aa, bB, Bb substrings. Define our F_2 to be the set of all reduced words $w \in \{a, b, A, B\}^*$. The operation here is
  - Concatenate, then
  - Delete aA, Aa, bB, Bb substrings until the string is reduced.

  Issue 1. Need to show this operation results in a unique reduced string.

  Issue 2. This assumes you have associativity.

Question: can you just define the operation from left to right? Answer: yes, this gives you uniqueness, but you have to show associativity.

Comment on this — you have to do a decent amount of work to rigorously show that you have $aba^{-1} \neq baab$. The idea of "conservation of difficulty.'

This is covered in section 6.3. Note that all the future homeworks will be hard (won't depend on chapters 1-6).

Consider $\mathbb{Z} = \langle x \rangle$. We also saw $\mathbb{Z}_5 = \langle x | x^5 = 1 \rangle$. Now, we can write $F_2 = \langle r, s \rangle$.

Note that we can write $D_{10} = \langle r, s | r^5 = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$. It is easy to check that all of these equalities hold, but the important take-away here is that all elements in D_{10} is a consequence of these three elements. Note that this fact implies that

$$n(D_{10}, G) = \left\{ (x, y) | x, y \in G, x^5 = 1, y^2 = 1, yxy^{-1} = x^{-1} \right\}$$

7 Lecture 11

Isomorphism theorems and quotient groups. Suppose you have a homomorphism

$$\alpha : G/N \to H.$$

Then you can get a homomorphism

$$a : G \to H$$

with $a(g) = \alpha(\overline{g})$.

Concretely, there is a bijection between homomorphisms $\alpha : G/N \to H$ and homomorphisms $a : T \to H$ with $N < \ker(a)$.

Suppose we have a group G, let $\overline{G} = G/N$. So we can define a projection π from $G \to G/N$. Suppose we have some subgroup $M < \overline{G}$. Claim: let $B = \pi^{-1}(M)$ be a subgroup of $\overline{G}$. Schematically, we can represent this as follows:

This implies that subgroups $\overline{B} \leq \overline{G}$ are in bijection with subgroups $N \leq B \leq G$. Additionally, we have $\overline{B} \cong B/N$.

If we have $N < B < C$ and $B \triangleleft C$, then we have that $\overline{C}/\overline{B} \cong C/B$.

This is a statement of the second / fourth isomorphism theorems $(-\epsilon)$.

Other way to write this isomorphism is to say $(C/N)/(B/N) \cong C/B$. One other thing we can check is that $\overline{A} \triangleleft \overline{G} \Leftrightarrow A \triangleleft G$.

7.1 Conjugation / conjugacy classes

Remember that we say that a is conjugate to b in G if there exists some g so that $b = gag^{-1}$.

Note that we can think of conjugation as a group action of the group G on the set $X = G$. Our definition here is

$$g * x := gxg^{-1}.$$

To check this is an action, we just need to check

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

Key thing we gain from thinking of this as a group action is that the conjugacy class of x is an orbit of x.

Corollary. The size of the conjugacy class of X divides $|G|$. More explicitly, the size of this conjugacy class equals the size of $|G|/|$stabilizer of $x|$. Definition: the stabilizer in this setting is called the "centralizer" subgroup (notation is $C_G(x)$).

- The definition of stabilizer: $\{g \in G | g * x = x\}$.
- The definition of orbit: $\{g \cdot x | g \in G\}$.

We are often interested in the size of some orbit. But instead, we can compute the fixed points. Note that each element x will have different centralizers.

This ends up implying the class equation. Let G be a finite group. Then we can write:

- $|G| = \sum$ size of each conjugacy class
- If there are k conjugacy classes in G, pick representatives $1, g_2, g_3, \ldots, g_k$. Then we can write
$$|G| = \sum_{i=1}^{k} [G : C_G(g_i)].$$
- If there are r conjugacy classes of size ¿ 1, say $g_1, \ldots, g_r$, then
$$|G| = \underbrace{|Z(G)|}_{\text{conjugacy classes of size 1}} + \sum_{i=1}^{r} [G : C_g(g_i)].$$

8 Lecture 12: Automorphisms and Sylow's Theorems

5B. Show that the commutator subgroup is not finitely generated. Call L the commutator subgroup of F_2, so that

$$L = \left\{ a^{k_1} b^{l_1} \ldots a^{k_n} b^{l_n} | \sum k_n = 0, \sum l_n = 0 \right\}.$$

The reason we call this L is to think about languages in computer sciences. Indeed, there is a notion of regular language (meaning it can be recognized by a finite state machine). This is a classic example of a language that is not regular.

Suppose L were finitely generated by a set, e.g. $\{aba^{-1}b^{-1}, aaba^{-1}\}\ldots$

The idea is that you can build a finite state automaton. This is not a DFA (but you can convert a non-deterministic automaton to a deterministic automaton.

Pumping Lemma. Idea: if you can produce longer and longer words, then it can't be regular. Importantly, to work on higher level math, you need to be able to "chunk" simple systems and apply "sub"-theorems.

Definition. *An automorphism of a group G is an isomorphism $f : G \to G$.*

Intuitively, we can think of the analogy bijection : permutation :: isomorphism : automorphism.

Definition. $\mathrm{Aut}(G)$ *is the group of automorphisms of G under composition.*

Proposition. *Let G be a group. Then $G/Z(G) \cong$ a subgroup of* $\mathrm{Aut}(G)$.

This is a strange statement, but it tells you a lot about how to prove it. When you see G/N is isomorphic to a subgroup H, immediately, you should think — I should produce a homomorphism $f : G \to H$ with $\ker(f) = N$. Since the first isomorphism theorem says that

$$G/\ker(f) \cong \mathrm{im}(f) \leq H.$$

Back to the proposition — we are looking for some homomorphism α with

$$\alpha : G \to \mathrm{Aut}(G)$$

with kernel $Z(G)$. You can think of this homomorphism as a group action. Since its kernel is $Z(G)$, we can write

$$Z(G) = \left\{zgz^{-1} = g \forall g\right\}.$$

So we can think of G acting on itself by conjugation, with $\alpha_g : G \to G$ with

$$\alpha_g(h) = ghg^{-1}$$

and

$$\ker(\alpha) = \{z \in G | \alpha_z = id\} = \left\{z | zhz^{-1} = h \forall h\right\} = Z(G).$$

Then, by the 1st isomorphism theorem

$$G/Z(G) = G/\ker(\alpha) \cong \mathrm{im}(\alpha) \leq \mathrm{Aut}(G).$$

Recall Euler's totient function, defined as

$$\phi(n) = \text{ of } 1 \leq k \leq n \text{ that are relatively prime to } n$$

Proposition. $\mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Recall $(\mathbb{Z}/n\mathbb{Z})^\times = \left\{\overline{k} \in \mathbb{Z}/n\mathbb{Z} | \overline{k} \text{ relatively prime to } n\right\}$, under multiplication.

For example,

$$\mathrm{Aut}(Z_8) \cong (\left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\right\}, \times).$$

And here, we have

$$\mathrm{Aut}(Z_8) = \left\{ f_1 : x^k \mapsto x^k, f_2 : x^k \mapsto x^{3k}, f_3 : x^k \mapsto x^{5k}, f_4 : x^k \mapsto x^{7k} \right\}.$$

Theorem. *(Non-obvious) Let p be an odd prime. Then $\mathrm{Aut}(Z_{p^k})$ is cyclic of order $\phi(p^k) = p^k - p^{k-1}$.*
Theorem. *(Non-obvious) For $p = 2$, note that $\mathrm{Aut}(Z_{2^k})$ is not cyclic, but its "almost cyclic":*

$$\mathrm{Aut}(Z_{2^k}) \cong Z_2 \times Z_{2^{k-2}}.$$

We will now change gears and discuss Sylow's theorem. We may not get to motivate why this is important, but it is very powerful.

Before class, for $G = S_4$, Church worked out the number of subgroups of S_4 of size k.

- $k = 1$, number of subgroups $N = 1$.
- $k = 2$, $N = 9$.
- $k = 3$, $N = 4$.
- $k = 4$, $N = 4$
- $k = 6$, $N = 0$.
- $k = 8$, $N = 3$
- $k = 12$, $N = 1$
- $k = 24$, $N = 1$.

The Sylow theorem is concerned with $k = 3$ and $k = 8$, since $|S_4| = 24 = 8 \cdot 3 = 2^3 \cdot 3$. Also, note the definition:
Definition. *A group P is called a p-group if $|P| = p^k$ for some $k \geq 0$.*

Definition. *Given a group G and a prime p, write $|G| = p^a \cdot m$ with $p \not| m$. A subgroup $P \geq G$ is called a Sylow p-subgroup if $|P| = p^a$.*

Definition. *Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G. Let $n_p(G)$ denote the number of Sylow p-subgroups of G.*

Theorem. *(Sylow's Theorem). Fix G and P.*

(1) *G has at least one Sylow p-subgroup (i.e. $n_p(G) \geq 1$).*

(2a) *Any two Sylow p-subgroups are conjugate. If $P_1 \leq G, P_2 \leq G$, with $|P_1| = |P_2| = p^a$, then there exist g such that $P_2 = gP_1g^{-1}$. In particular, they are all isomorphic to the others!*

(2b) *Any p-subgroup is contained in some Sylow subgroup. If $Q \leq G$ and $|Q| = p^b$, there exists some $P \leq G$ with $|P| = p^a$ and $Q \leq P$.*

(3) *We know that $n_p(G) \equiv 1 \pmod{p}$ and $n_p(G)$ divides m.*

For example, if $|G| = 11 \cdot 5^{100}$. Then the number $n_p(G) \equiv 1 \pmod 5$ and divides 11. This tells us $n_5(G) = 1$ or 11.

If $|G| = 7 \cdot 5^{100}$. This tells us $n_5(G) \equiv 1 \pmod 5$ and it divides 7, so $n_5(G) = 1$.

Corollary. G has a unique Sylow p-subgroup if and only if G has a normal Sylow p-subgroup if and only if $n_p(G) = 1$.

Why are these equivalent? If there is only one subgroup that that size, then imagine conjugating it. Clearly $|P| = p^k$, and $|gPg^{-1}| = p^k$, which implies that they are the same subgroup, and that it is normal. (The converse is straightforward too).

9 Lecture 14

Lemma A. For any G with $|G| = p^k m > 1$ ($p \not| m$), either

- G has a subgroup $H \not\leq G$ with $|H| = p^k l < p^k m - |G|$.
- G has a quotient $G \to \overline{G}$ with $\overline{G} = p^b m < p^k m = |G|$.

For any $H \leq G$, we can consider action of H on the set of subsets of G by conjugation.

That is,

$$S \mapsto hSh^{-1} = \left\{hsh^{-1} | s \in S\right\}.$$

Write $\Theta_H(S) =$ orbit of S, $\Theta_H(S) = \{hSh^{-1} | h \in H\}$.
Proposition. *(B.) Let R be a p subgroup of G. Then let Q be any p subgroup of G.*

- $|\Theta_Q(R)| = 1$*, if and only if* $Q \subseteq R$.
- *Otherwise,* $|\Theta_Q(R)| \equiv 0 \pmod p$.

From this, we are going to prove Sylow's Theorem.

Proof. (Proof of Sylow (i) using Lemma A.)

By induction on $|G|$. Base case $|G| = 1$. Inductive step, consider Lemma A.

- If there exists $H \leq G$, with $|H| = p^k l < p^k m = |G|$. By induction, H has a p subgroup with $|P| = p^k$, so there exists a p-Sylow subgroup.
- If $\pi : G \to G$ with $|\overline{G}| = p^b m < p^k m = |G|$. Let $N = \ker(\pi)$, and set $\overline{G} \cong G/N$. Then $|\overline{G}| = |G|/|N|$, and we can write $p^k m = p^k m/|N|$.

  By induction, $\overline{G}$ has a p-Sylow subgroup $\overline{P}$. Set $P = \pi^{-1}(\overline{P})$. Then

$$|P| = |\overline{P}||N| = p^b \cdot p^{k-b} = p^k.$$

□

We now proceed to prove Sylow (3) using Prop B:

Proof. Let $P_1, P_2, \ldots, P_{n_p}$ be all the p-Sylow subgroups of G, and suppose P is a p-Sylow.

Consider the p-orbits on $P_1, \ldots, P_{n_p}$ acting by conjugation. Apply Proposition B with $Q = P$ and $R = P_i$. Now,

- $|\Theta_p(P_i)| = 1$ if and only if $P \subseteq P_i$ but $P = P_i$ b/c $|P| = |P_1| = p^k$.

Now, we just need to know that n_p divides $|G|$. Because then we have $n_p | p^k m$ and $p \not| n_p$, which implies that $n_p | m$. Then $n_p || G|$ follows from Sylow 2(a), since given 2(a), $n_p =$ size of the orbit under conjugation by G. □

We now proceed to prove Sylow (2b):

Proof. Let Q be any p-subgroup of G. Suppose for a contradiction that Q is not contained in any p-Sylow subgroup.

Consider the Q-orbits on $P_1, \ldots, P_{n_p}$. By proposition B, this assumption implies that all of the orbits have size $\equiv 0 \pmod{p}$.

Examining the list, we can break this into

$$\{P_1, \ldots, P_k\}, \ldots, \{P_k, \ldots, P_{n_p}\},$$

which implies that $n_p = 0 + \cdots + 0 \pmod{p}$, which contradicts $n_p \equiv 1 \pmod{p}$. □

Note that we can also get a corollary ("2b + ϵ"). In fact, the number of p-subgroups contained in Q is $\equiv 1 \pmod{p}$.

We now will prove (2a) using Proposition B.

Proof. Let $c =$ of conjugates of P, and let $P_1, P_2, \ldots, P_c$ be the G-conjugates of P, with $P = P_1$. Similarly, we can look at any group acting on the list $P_1, \ldots, P_c$.

If we first consider P acting on this list by conjugation, then we get that it splits up into something like:

$$\{P_1\}, \{\ldots\}, \ldots, \{\ldots, P_k\},$$

where $c = 1 + 0 + \cdots + 0 \pmod{p}$.

Now, asume for contradiction that L is a p-Sylow that is not conjugate to P. Then L is not in this list. Look at the L-orbits; the only possible size 1 orbits would be if e.g. $L = P_7$ (L has to be equal some element in this list). But we just assumed that L is not in this list, so there is no size 1 orbits, but this gives $c \equiv 0 \pmod{p}$, which is a contradiction. □

Aside: we can use this to show that every matrix mod p whose order is a power of p has an eigenvector with eigenvalue 1.

10 Lecture 15

Lemma C. If R is a p-Sylow subgroup of G, with $G = p^k m$, and $q \in G$ has $|q| = p^b$, then $qRq^{-1} = R$ iff $q \in R$ (conjugation is the trivial map).

Proposition B. Let R be a p-Sylow subgroup of G, and let Q be any p-subgroup of G. Then $||\Theta_Q(R)| = 1$ iff $Q \subseteq R$, otherwise $|\Theta_Q(R)| \equiv 0 \pmod p$, and $|\Theta_Q(R)| =$ number of Q conjugates of R.

Note that Lemma C implies Proposition B. (This is not that hard of a proof).

Lemma D. For any G, and any $H \leq G$, if $gHg^{-1} = H$, then $K = \left\{g^k h | k \in \mathbb{Z}, h \in H\right\}$ is a subgroup of G, and it's $\langle g, H\rangle$.

Proof that Lemma D implies Lemma C. (In the case where $|q| = p$.) Set $K = \left\{q^k r | k \in \mathbb{Z}, r \in R\right\}$. Lemma D tells us that this is a subgroup. We now consider its size. Now, since $|q| = r$, we can write

$$K = \left\{q^k r | k \in \{0, \ldots, p-1\}, r \in R\right\}.$$

Suppose that $q \notin R$, for a contradiction. This implies that $q^k \notin R$ for $k \in \{1, \ldots, p-1\}$. This implies that the cosets $R, qR, q^2R, \ldots, q^{p-1}R$ are all disjoint (this statement requires some thought, think about it). This implies that the size of the set $K = p \cdot |R| = p^{k+1}$. No subgroup of b has size p^{k+1}, since it does not divide the order of the group.

Proof of Lemma D. We just need to check that this set is closed under multiplication / inverses. Choose two elements $a, b \in K$. We can write $a = q^k h_1$, $b = q^l h_2$. Then we can write $ab = q^k h_1 q^l h_2$. Now, $h_3 = q^{-l} h_1 q^l \in H$. Some substitution / algebra gives us $ab = q^{k+l} h_2 h_3 \in K$, so that K is closed under multiplication.

Broader point of Lemma D. For all $h_1 \in H, g$, there exists some h_3 such that $gh_1 = h_3 q$.

2nd Isomorphism Theorem Now, suppose $A \leq G, B \leq G$, and suppose $aBa^{-1} = B$ for all $a \in A$. Then the set

$$AB = \{ab | a \in A, b \in B\}$$

is a subgroup and it's $\langle A, B\rangle$. Note that the proof ends up being exactly the same as before.

And furthermore:

- $B \trianglelefteq AB$
- $A \cap B \trianglelefteq A$
- $AB/B \cong A/A \cap B$.

Note: $|AB| = \frac{|A||B|}{|A \cap B|}$. [5]

We can write down a helpful definition:

[5] Note that this is true even without the assumption that $aBa^{-1} = B$ for all a, i.e. even when AB is not a subgroup, it still has this size.

Definition. *For any subset $H \leq G$, the normalizer $N_G(H)$ is* $N_G(H) = \{g \in G | gHg^{-1} = H\}$.

Proposition. (5.4.9) Suppose you have two normal subgroups $N \triangleleft G$, $H \trianglelefteq G$, $N \cap H = 1$. Then $NH \cong N \times H$.

Corollary. If $|G| = 15$, then $G \cong Z_3 \times Z_5$.

Proof sketch. We know that there's a bijection between NH and $N \times H$, just by writing $\{nh\} \mapsto (n, h)$. Need to show: for all $n \in N$ and $h \in H$, we need to show that n and h commute (implies that this bijection is an isomorphism).

We know this because $hn = nh$ is the same as $n^{-1}h^{-1}nh = 1$. We can write

$$\underbrace{n^{-1}}_{\in N}\underbrace{h^{-1}nh}_{\in N} = \underbrace{n^{-1}h^{-1}n}_{\in H}\underbrace{h}_{h \in H} \in \{1\}.$$

Now, suppose $N \trianglelefteq G$, $H \leq G$, $N \cap H = \{1\}$. Then every $g \in G = NH$ uniuqely written as

$$g = nh$$

where

$$G = NH \text{ is a bijection with } N \times H$$

but it is not an isomorphism because $nhnh^{-1}$ can be viewed as $H \to \mathrm{Aut}(N)$.

This is the only infomration that is necessary to remember what G is.

Question 7 can be rephrased as: suppose you have some action from $H \to \mathrm{Aut}(N)$, you can define a group G whose elements are pairs (n, h) with

$$(n_1, h_1)(n_2, h_2) = (n_1(h_1 * n_2), h_1h_2),$$

where we are thinking of $*$ as the action. This is the semi direct product of N and H.

11 Lecture 18

In this lecture, we'll discuss examples of rings to have in mind. Note that the operations can in principle be "strange" and not be usual addition / multiplication (see Question 0 on homework), but typically the operations will be canonical. "Main" examples of rings are like: $\mathbb{Q}, \mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}$.

- Fields, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2})$[6], $\mathbb{F}_p$
- Integers
- Modular stuff: $\mathbb{Z}/n\mathbb{Z}$ (won't write Z_n).
- Polynomials. We can write

$$\mathbb{Z}[x] = \left\{a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 | a_i \in \mathbb{Z}, n \geq 0\right\}$$

[6]Subfield of $\mathbb{R}$ generated by $\mathbb{Q}$ and $\sqrt{2}$

More examples: we can write

$$\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} | a, b \in \mathbb{Z}\right\}$$
$$\mathbb{Z}[\sqrt[3]{2}] = \left\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 | a, b, c \in \mathbb{Z}\right\}.$$

Note that if A and B are rings, $A \times B$ is a ring with

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \times (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Consider the ring of "functions of something." For example,

$$C([0, 1]) = \{\text{continuous functions } f : [0, 1] \to R\}.$$

Can consider various extensions of this theme:

$$\begin{aligned} C([2, 7]) &= \{\text{continuous functions } f : [2, 7] \to R\} \\ &\ldots = \{\text{infinitely differentiable functions } f : [0, 1] \to R\} \\ &\ldots = \{\text{continuous functions } f : [0, 1] \to \mathbb{C}\} \\ &\ldots = \{\text{functions } f : [0, 1] \to R\} \end{aligned}$$

It turns out that these examples are the "most canonical" in some sense (but this requires theory to explain). One important idea is to consider rings that are restrictions of larger rings. For example, let $f \in \mathbb{C}([0, 10])$. We can consider the ring of functions restricted to $[4, 6]$. It turns out that

$$r : C([0, 10]) \to C([4, 6])$$

is a ring homomorphism.

Grothendieck won a Fields medal for constructing a "something" so you can consider any ring as functions on "something."

Definition. *We say $r \in R$ is a unit if it has a multiplicative inverse. We write*

$$R^\times = \{\textit{units } r \in R\}.$$

Definition. *A ring R is a field if $0 \neq 1$ and $R^\times = R - \{0\}$, i.e. every nonzero element is a unit.*

Recall key idea from linear algebra. Suppose you have an equation $ax + by = 0$, where $a \neq 0$. In a field, this would imply that $x + a^{-1}by = 0$. This is useful, but it isn't possible in general (even in the integers).

Now, over the integers, suppose we had the equation $2x+3y = 0$. We could not write $x+\frac{3}{2}y = 0$. However, we can divide in certain cases; if $10x = 10y$, then $x = y$.

Definition. *We say $r \in R$ is a zero-division if $r \neq 0$ and there exists $s \neq 0 \in R$ such that $r \cdot s = 0$.*
Example. *If $\mathbb{Z}/10\mathbb{Z}$, $r = 4$, $s = 5$, so that $rs = 20 = 0 \in \mathbb{Z}/10\mathbb{Z}$.*

Definition. *A commutative ring R is a domain if $0 \neq 1$ and it has no zero-divisors.*

Proposition. *If R is a domain, if $a \neq 0$, then $ax = ay$ implies $x = y$.*

In the examples we described, all the fields are domains. Also, a given $r \in R$ can't be both a unit and a zero-divisor. To see this, suppose we had $rs = 0$, with $s \neq 0$, but also $r^{-1}r = 1$. Then left multiplying by r^{-1}, we get $r^{-1}rs = 0$, implying $s = 0$, which is a contradiction.

We now turn to the definition of a ring homomorphism.
Definition. *If A, B are rings, a function $f : A \to B$ is a (ring) homomorphism if:*

- $f(1) = 1$
- $f(a + b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$.

Definition. *Let R be a ring, and suppose $A \subseteq R$ is a subset of R. We say A is a subring of R if*

- $1 \in A$
- *A is a subgroup under addition*
- *A is closed under multiplication*

Caution: the book lies. (About point 1 of the previous two definitions). E.g. the book will say $2\mathbb{Z}$ is a subring, but it is not, because it doesn't contain 1.

12 Lecture 20

We start be discussing the isomorphism theorems for rings.

1. Recall the first isomorphism theorem for rings from last lecture that says

$$\mathrm{im}(f) \cong R/\operatorname{Ker}(f); \quad f : R \to S.$$

2. Suppose A is a subring of R, and I is an ideal of R. Then

$$A + I = \{a + i | a \in A, i \in I\} \text{ is a subring}$$

$$A \cap I \text{ is an ideal of } A$$
$$\frac{A + I}{I} \cong \frac{A}{A \cap I}.$$

This basically parallels the second isomorphism theorem for groups, except that they call it N instead of I. Don't worry too much about the raw intuition of this one, focus on seeing lots of examples.[7]

3. (3rd + 4th) Fix $I \subseteq R$ an ideal. We saw last time that we have this map $R \to R/I = \overline{R}$. We claim that there is a correspondence between ideals $J \subseteq R$ containing I and ideals $\overline{J} \subseteq \overline{R}$. In particular, we can write

$$R/J \cong \overline{R}/\overline{J} = (R/I)/(J/I).$$

It's also true that subrings $S \subseteq R$ containing I are in bijection with subrings $\overline{S} \subseteq \overline{R}$, where $\overline{S} = S/I$.

Here's another (easier) way to keep track of what this is saying. Suppose you want to define some homomorphism $\overline{f} : R/I \to C$. What would be great is if there was some function $f : R \to C$, so we can just write $\overline{f}(\overline{r}) = f(r)$. The question is: when is this actually well defined? We need that $\overline{f}$ needs to be equal for all representatives mod I. In particular, we need $0 = \overline{f}(0) = \overline{f}(\bar{i}) = f(i)$. The theorem is saying in particular that this is all you need! In particular:

$$\left\{\text{homomorphisms } \overline{f} : R/I \to C\right\} \Leftrightarrow \{\text{homomorphisms } f : R \to C, f(I) = 0\}$$

The rest of today will be spent on definitions, which will help to make a lot of this concrete. [8]

Let's now talk about generators.

Definition. *Suppose you have a subset $X \subseteq R$. We write (X) to denote the ideal of R generated by X. If X is finite, with $X = \{x_1, \ldots, x_k\}$, write*

$$(X) = (x_1, \ldots, x_k).$$

There are two definitions here that we can state:

- *(X) is the smallest ideal containing X, namely*

$$X = \bigcap_{\text{ideal } I, X \subseteq I} I$$

- *(X) is the set of all linear combinations of arbitrary length:*

$$(X) = \{r_1 x_1 + \cdots + r_n x_n | n \in \mathbb{N}, r_i \in R, x_i \in X\}.$$

[7] When do we see the second isomorphism theorem? We used the group analog a lot with identities like $|HN| = \frac{|H||N|}{|H \cap N|}$. Say we were thinking about vector spaces. We would say something like $\frac{V+W}{W} \cong \frac{V}{V \cap W}$, where V, W are subspaces of X. Suppose we had some $f : X \to Y$ with $\ker(f) = W$, then both sides are isomorphic to $f(V)$. In particular, we can obtain $f(V + W) = f(V)$. Check out https://math.stackexchange.com/questions/1738334/intuition-about-the-second-isomorphism-theorem

[8] "Comment that is maybe too enlightened": even if we hadn't defined this previous bijection, you could take this bijection as the definition of R/I; and the answer is that you don't *need* to know exactly which set it is, just need to know where things map.

Definition. *Consider the subring S of R generated of X. We can write*

- *S is the smallest subring of R containing X:*

$$S = \bigcap_{A, X \leq A} A.$$

- *You can also write*

$$S = \left\{ \sum_{i=1}^{n} \prod_{j=0}^{m_i} x_{ij} \mid x_{ij} \in X, m_i \geq 0 \right\}.$$

In particular, we can take the empty product to that 1 is in the subring S..

Further, note that if I is generated by some subset X, so that $I = (X)$, we can define an equality

$$\{\text{homomorphisms } f : R \to C, f(X) = 0\}$$
$$= \left\{\text{homomorphisms } \overline{f} : R/I \to C\right\} \Leftrightarrow \{\text{homomorphisms } f : R \to C, f(I) = 0\}$$

Example. Consider the following ring. Let $R = \mathbb{Q}[x, y]$, that is linear combinations of $x^i y^j$. We say that I is a principal ideal if it is generated by one element. In particular, let $I = (x^2 + y^2 - 1)$, and $A = R/I$. Question: how many homomorphisms $\phi : A \to \mathbb{Q}$ are there? Note that $\mathbb{Q} \subset A$ are the constrant polynomials, so that $\phi(x) = x$ for any $x \in \mathbb{Q}$ (since you have to take $1 \to 1$).

This is a great advertisements for the bijections mentioned previously! It is really hard to write up an explicit homomorphism from first principles. But it turns out that the answer is

$$\left\{ \text{ of pairs of numbers } a, b \in \mathbb{Q} \text{ with } a^2 + b^2 = 1 \right\}.$$

This hints at why rings are useful. It means that we can encode solutions to polynomial equations in terms of homomorphisms from sonme ring. Just like group theory in some sense is based on understanding symmetric groups, ring theory is based on understanding solutions to equations.

Question: can you apply this argument to encode solutions to equations over other fields? Yes. One caveat is that if you are working over F_n for some composite n, you have to specify the constant mapping explicitly, i.e.

$$\phi : \mathbb{F}_n[x, y]/(I) \to \mathbb{F}_n; \qquad \phi(c) = c; \forall c \in \mathbb{F}_n.$$

This starts to hint at why algebraic geometry, number theory, and ring theory are fundamentally intertwined. Note that there's a fantastic theorem proved by Hasse.

Hasse Local-Global Primes. Let's say you have a function $f(x, y, z, w) =$ quadratic in the inputs. Hasse says that $f(x, y, z, w) = 0$ has a solution in the integers if and only if $f(x, y, z, w) = 0$ has

a solution in $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z}\ldots$ for all primes p, and has a solution in the reals. Check out Keith Conrad's article on this[9].

We continue to some basic definitions.
Definition. *An ideal $P \not\subseteq R$ is a prime ideal if $a \cdot b \in P$ implies $a \in P$ or $b \in P$.*[10]
Definition. *Let $M \subseteq R$ with $M \neq R$ is a maximal ideal if it's maximal. That is, there doesn't exist I with $M \not\subseteq I \not\subseteq I$. Note that maximal ideals are prime.*

[9] http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/localglobal.pdf

[10] Note that this is a property of prime numbers. $p = (5)$ is prime, since if $ab \equiv 0 \pmod 5$ then $a \equiv 0 \pmod 5$ or $b \equiv 0 \pmod 5$. Note that this isn't the same as not having factors other than 1 and p.

13 Lecture 23

Fix a field F and let $R = F[x]$. Claim: R is a PID. Given ideal $I \subseteq R$, let $m_I \in I$ be the monic polynomial in I of smallest degree. Then I is generated by m_I, i.e. $I = (m_I)$.

14 Lecture 29

Today, we'll discuss: what is $i \in \mathbb{Z}/5^\infty\mathbb{Z}$? Recall that:

$$(\mathbb{Z}/5^k\mathbb{Z})^\times \equiv \mathbb{Z}_{5^k - 5^{k-1}} \equiv \mathbb{Z}_{4\cdot 5^{k-1}},$$

so there exists four solutions to $x^4 = 1$ in $\mathbb{Z}/5^k\mathbb{Z}$, that is, $1, -1, a \equiv 2 \pmod 5, a \equiv 3 \pmod 5$.

We want: an algorithm / procedure to compute a. Question: how would Newton compute $\sqrt{2} \in R$? One application of his calculus is an algorithm to compute roots of polynomials. Suppose we are trying to find the roots of $f(x) = 0$.

- Start with an initial guess, e.g. $a_1 = 10$.
- Take a linear approximation to the function $f(x)$. This is a line through $(a_1, f(a_1))$, with slope $f'(a_1)$. Set the next guess to the be x-intercept, $a_2 = a_1 - \frac{f(a_1)}{f'(a_1)}$.
- Repeat the update rule $a_k = a_{k-1} - \frac{f(a_{k-1})}{f'(a_{k-1})}$ until convergence.

Coming back to the infinite integers, we try to find solutions of $x^2 = -1$.

- Initial guess $a_1 = 2$.
- $a_2 = a_1 - \frac{f(a_1)}{f'(a_1)} = 2 - \frac{5}{4} = \ldots 1112$.

Note, we can write

$$-\frac{1}{4} = \ldots 1111$$
$$-\frac{5}{4} = \ldots 1110$$
$$2 + (-\frac{5}{4}) = \ldots 1112$$

Similarly, we can write

$$\frac{1}{7} = \ldots 1033$$
$$\frac{25}{7} = \ldots 103300$$
$$-\frac{25}{7} = \ldots 341200$$

$$7 - \frac{25}{7} = \ldots 341212.$$

To show that this converges, we just need to argue that this will give us one more digit each time.

Suppose $f(x) \in (\mathbb{Z}/5^\infty\mathbb{Z})[x]$. Take the initial guess a_1 such that $f(a_1) \equiv 0 \pmod 5$ and $f'(a_1) \not\equiv 0 \pmod 5$. Claim: if you define $a_{k+1} = a_k - \frac{f(a_k)}{f'(a_k)}$, then

$f(a_k) \equiv 0 \pmod{5^k}$ (i.e. the last k digits are 0).

Note: this implies a_{k+1} and a_k have the same last k digits. In the context of convergence, this is like saying that the difference between two successive terms is getting smaller and smaller.

The convergence test for a series is just: do the terms go to 0? But this isn't true in calculus, since the harmonic series diverges.

Let's do what Newton would do and plug in $f(a_{k+1})$. We are hoping that $f(a_{k+1}) \equiv 0 \pmod{5^{k+1}}$. We can write

$$f(a_{k+1}) = f(a_k - \frac{f(a_k)}{f'(a_k)}) = f(a_k + h) = f(a_k) + hf'(a_k) + O(h^2).$$

We know here that $h \equiv 0 \pmod{5^k}$, so $h^2 \equiv 0 \pmod{5^{2k}}$, and certainly $h^2 \equiv 0 \pmod{5^{2k+1}}$.

Therefore,

$$f(a_{k+1}) \equiv f(a_k + h) \equiv f(a_k) + hf'(a_k) \pmod{5^{k+1}}$$
$$f(a_k) - \frac{f(a_k)}{f'(a_k)} f'(a_k) \equiv 0 \pmod{5^{k+1}}.$$

Note that this argument works for any prime p, not just 5.

And furthermore, this implies that a_k is a well defined element $a_\infty \in \mathbb{Z}/p^\infty\mathbb{Z}$ with $f(a_\infty) = 0$. This is called Hensel's Lemma.

Here's another formulation of Hensel's Lemma (which happens to be a bit stronger). Consider some $f(x) \in (\mathbb{Z}/5^\infty\mathbb{Z})[x]$. Something we could do is to drop everything after the last coefficient. There's a ring homomorphism from $(\mathbb{Z}/5^\infty\mathbb{Z})[x] \to (\mathbb{Z}/5\mathbb{Z})[x]$.

If there exists a_1 such that $\overline{f}(\overline{a_1}) = 0$ and $\overline{f}'(\overline{a_1}) \neq 0$, then we can write

$$\overline{f}(x) \text{ factors as } \overline{f}(x) = (x - \overline{a_1})\overline{g}(x)$$
$$\overline{g}(x) \text{ not divisible by}$$

x - $\overline{a_1}$.

Theorem (Strong Hensel's Lemma). *Given a monic polynomial $f(x) \in \mathbb{Z}/5^\infty\mathbb{Z}[x]$, if $\overline{f}(x)$ factors into monic coprime $\overline{g_i}(x)$, $\overline{f}(x) = \overline{g}_1(x) \ldots \overline{g}_k(x)$, then there exists monic coprime $g_i(x) \in (\mathbb{Z}/5^\infty\mathbb{Z})[x]$ such that $f(x) = g_1(x) \ldots g_k(x)$.*

15 Notes on Group Actions

Let G be a group acting on a nonempty set A. Recall that a group action must satisfy the following properties:

- $g_1 \cdot (g_2 \cdot a)$ for all $g_1, g_2 \in G$, $a \in A$ and
- $1 \cdot a = a$ for all $a \in A$.

Note that for each $g \in G$, the map $\sigma_g : A \to A$ defined by $a \mapsto g \cdot a$ is a permutation of A. To see this, note that σ_g has a two sided inverse (follows from the first condition above). Note also that there is a homomorphism associated to an action of G on A:

$$\varphi : G \to S_A; \qquad \text{defined by } \varphi(g) = \sigma_g,$$

called the permutation representation associated to the given action. We note some basic definitions:

1. The *kernel* of an action is $\{g \in G | g \cdot a = a\}$.
2. The *stabilizer* on a in G is $\{g \in G | g \cdot a = a\}$, denoted by G_a.
3. An action is *faithful* if its kernel is the identity.

The kernel of an action is a normal subgroup of G. An action of G on A may also be viewed as a faithful action of the quotient group $G/\ker\varphi$ on A.

16 Notes on Irreducibility

Eisenstein's. Let p be a prime in and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Suppose $p|a_i$ for $i \in \{0, 1, \ldots, n-1\}$ but $p^2 \not| a_0$. Then $f(x)$ is irreducible in both $[x]$ and $[x]$.

Generalized Eisenstein's. Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in $R[x]$. Suppose $a_{n-1}, \ldots, a_1, a_0$ are elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.

(p 312). $x^{n-1} + \cdots + x + 1$ is irreducible if and only if n is prime.

(p 315). $x^n - p$ is irreducible over $\mathbb{Z}[i]$.

17 Notes on Free Groups

18 Key Ideas

18.1 Definitions

Definition. *A binary operation $*$ on a set G is a function $* : G \times G \to G$.*

Definition. *A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:*

1. *$\star$ is associative*
2. *There exists an element e in G, such that $a \star e = e \star a = a$ for all $a \in G$.*
3. *For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.*

Definition. *A group $(G, \star)$ is called abelian if $a \star b = b \star a$ for all $a, b \in G$.*

Definition. *Let F be a field. Then $GL_n(F)$ is*

$$GL_n(F) = \{A | A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\}.$$

Definition. *Let $(G, *)$ and $(H, \circ)$ be groups. A map $\psi : G \to H$ such that*

$$\psi(x * y) = \psi(x) \circ \psi(y) \text{ for all } x, y \in G$$

is called a homomorphism.

Definition. *The map $\psi : G \to H$ is called an isomorphism if*

1. *ψ is a homomorphism*
2. *ψ is a bijection*

Definition. *A group H is cyclic if H can be generated by a single element.*

Definition. *A function $f : A \to B$ is injective if $f(x) = f(y)$ implies $x = y$. f is surjective if for all $b \in B$, there exists some $a \in A$ with $f(a) = b$.*

Definition. *A subgroup N is called normal if it is invariant under conjugation. In other words:*

- *For all g, $gH = Hg$.*
- *For all g, $gNg^{-1} = N$.*
- *There is some homomorphism on G for which N is the kernel. Intuition: consider the map $\pi(g) = gN$ for all ga This homomorphism is called the "natural projection" of G onto G/N.*

18.2 Propositions and Theorems

Proposition. *A subset H of a group G is a subgroup if and only if:*

1. *$H \neq \emptyset$ and*
2. *for all $x, y \in H$, we have $xy^{-1} \in H$.*

18.3 Examples

Example. *The number of homomorphisms from $\mathbb{Z}_m \to \mathbb{Z}_n$ is $\gcd(m, n)$.*

18.4 Ideas

1. To show a mapping is a homomorphism, first show that the mapping is well-defined ($b_1 = b_2$ implies $f(b_1) = f(b_2)$). Then, show that f is a homomorphism, that is $f(g_1 g_2) = f(g_1)f(g_2)$.
2. Studying quotient groups of G is equivalent to the study of the homomorphisms of G.

19 Things to review

1. Proof of Sylow's theorem.
2. More intuition for conjugation.
3. Book sections.