MATH 3113 Notes #1

Dr. Day

1/14/19

1 Prerequisites

1.1 Mathematical proficiency

This is a proof-based course on group theory and ring theory. To do well in this course, you need to be proficient with the following things, which you should have seen in previous courses.

- Using predicate logic. This includes:
  - truth tables for logical connectives,
  - use of quantifiers,
  - dummy variables,
  - scope of variables, and
  - logical laws.
- Writing short proofs. This includes:
  - introducing terms,
  - structuring proofs (for many proofs, the structure of the proof mirrors the structure of the statement being proven),
  - following your nose to complete an argument, and
  - using semi-formal language.
- Reading and thinking about mathematics. This includes:
  - unpacking definitions,
  - recognizing instances of definitions,
  - problem-solving,
  - building and working with examples, and
  - checking and formalizing arguments.

1.2 Basic set theory

You will also need to be able work with the following concepts from set theory:

- set membership,
- proving and exploiting subset inclusion ($A \subset B \iff \forall x \in A, x \in B$),
- proving and exploiting set equality ($A = B \iff A \subset B$ and $B \subset A$),
- using set-builder notation (like $\{x \in X | P(x)\}$), and
- using set operations ($\cup, \cap, \setminus, \times$).

1.3 Functions and equivalence relations

We will assume knowledge of functions and equivalence relations. These are explained nicely in sections 2.1 and 2.2 of the textbook.

2 Preview of group theory

2.1 Motivating the group definition

In the first part of this course we will study group theory. These notes preview the important concepts; we will study each one in detail later. In particular, we omit the formal definitions here.

The concept of a *group* is supposed to unify many examples of algebraic structures from around mathematics. A group is a set, together with an algebraic sum or product operation satisfying certain properties.

A first example is the integers $\mathbb{Z}$ with addition $+$. This is a set together with an algebraic operation. Really, $+$ is a function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$, although we write it as $x + y$ instead of $+(x, y)$. The operation $+$ has many nice properties.

A second example is multiplication of invertible matrices. Fix a positive integer n and let $\mathrm{GL}_n(\mathbb{R})$ be the set of all invertible $n \times n$ matrices with entries in $\mathbb{R}$. For $A, B \in G$, let $A \cdot B$ be the usual matrix product of A and B (take the dot products of the rows of A with columns of B, and arrange them in an $n \times n$ matrix). Again, $\cdot$ is really a function from $\mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{R})$ to $\mathrm{GL}_n(\mathbb{R})$. This $\cdot$ also has many nice properties, but not the same properties as $+$ on $\mathbb{Z}$.

In both examples, we can do algebra. We can take sums of multiple integers, and we can take products of multiple matrices. We can solve equations involving sums of integers, and we can solve equations involving products of matrices. Being able to do these things comes from two properties: *associativity*, and the existence of *inverses*.

Associativity means that order of operations does not matter, and finite products are unambiguous. When adding integers, $(x + y) + z = x + (y + z)$, so we might as well write $x + y + z$. The placement of parenthesis does not matter, so order of operations does not matter. By iterating this, it follows that

for a finite sum of integers, we can just list the integers involved, and ignore the parenthesis. Write $1+2+(-3)+5$ instead of $1+((2+(-3))+5)$.

Do not confuse associativity with commutativity. Commutativity says that order does not matter; associativity says that order of operations does not matter, even though order might matter. Notice that in $\mathbb{Z}$, order doesn't matter, but in $\mathrm{GL}_n(\mathbb{R})$, order sometimes matters. In $\mathrm{GL}_2(\mathbb{R})$, we have

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\neq\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

However, $\mathrm{GL}_n(\mathbb{R})$ is still associative, since for any three $n\times n$ matrices A, B, and C, we definitely have $(A\cdot B)\cdot C=A\cdot(B\cdot C)$.

An example of an algebraic structure that is not associative is the integers with subtraction as an operation. Note that $(1-1)-1=-1\neq 1=1-(1-1)$. Since subtraction is not associative, it is not meaningful to take the difference of a big finite sequence of integers.

Now we consider solving equations. If I want to solve $2+x=1$ in $\mathbb{Z}$, I have to know that there is something I can add to $2+x$ to undo the effect of adding 2 to x. So I add -2 to both sides: $-2+2+x=-2+1$; and I simplify: $x=-1$. This has a name: -2 is the *inverse* of 2 (really, the *additive inverse*). If we operate by something, and then by its inverse, then this is the same as doing nothing.

Matrices in $\mathrm{GL}_n(\mathbb{R})$ also have inverses, and we can solve simple matrix equations like

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot A=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix},$$

in the same way, by multiplying both sides of the equation on the left by the inverse of the appropriate matrix (here $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}$).

An example of an algebraic structure without inverses is positive integers $\mathbb{Z}_+$ with addition $+$. We cannot solve $2+x=1$ in $\mathbb{Z}_+$ by the method above, and in fact, it has no solution in $\mathbb{Z}_+$.

We summarize the group definition as follows: a group is a set together with a product or sum operation, such that the operation is associative, and every element has an inverse. So in a group, order of operations does not matter (although order might matter), and whatever we do by operating by an element, we can undo it by operating by its inverse element. Under this definition, $\mathbb{Z}$ with $+$ and $\mathrm{GL}_n(\mathbb{R})$ with $\cdot$ are both groups, but $\mathbb{Z}$ with $-$ and $\mathbb{Z}_+$ with $+$ are not groups.

(Later we will also talk about the *identity element* when we define groups. This is an element where operating by this element does nothing. We don't include that in our definition here, because its existence is implied by the existence of inverses.)

2.2 Functions between groups

In set theory, we consider functions between sets. In group theory, we consider functions between groups. However, most functions between groups are messy: usually, considering a function from one group to another doesn't help you do algebra in either group. We are interested in special functions that respect group structure; these are called *homomorphisms*.

Here is an example. Define $\phi\colon \mathbb{Z} \to \mathrm{GL}_2(\mathbb{R})$ by

$$\phi(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Notice that ϕ respects $+$ and $\cdot$, since for any n and m in $\mathbb{Z}$, we have

$$\phi(n) \cdot \phi(m) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = \phi(n+m).$$

This makes ϕ an example of a homomorphism. This means that we can compute in $\mathbb{Z}$ (which is easier) instead of computing in $\mathrm{GL}_2(\mathbb{Z})$ (which is harder) whenever we are interested in doing computations in the image $\phi(\mathbb{Z})$.

Contrast this to the function $f\colon \mathbb{Z} \to \mathrm{GL}_2(\mathbb{R})$ given by

$$f(n) = \begin{pmatrix} \frac{1}{2} + n & 0 \\ 0 & 1 \end{pmatrix}.$$

Notice that

$$f(n) \cdot f(m) = \begin{pmatrix} \frac{1}{4} + \frac{1}{2}(n+m) + nm & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{and}$$

$$f(n+m) = \begin{pmatrix} \frac{1}{2} + n + m & 0 \\ 0 & 1 \end{pmatrix},$$

and therefore $f(n+m) \neq f(n) \cdot f(m)$ for integers n and m. So f is not a homomorphism. In particular, using f doesn't help us compute in either group. This is what typically happens with functions between groups.

The homomorphism ϕ we gave above has an extra nice property: it is injective. Many homomorphisms are not injective. However, ϕ is not surjective. (Why?) Bijective homomorphisms are particularly nice, and we can fix ϕ and make it into a bijective homomorphism by changing its codomain.

Define

$$H = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) | n \in \mathbb{Z}\},$$

and put $\cdot$ on H as an operation. It turns out that H is a group. (So $\cdot$ is a well defined associative operation on H, and every element of H has an inverse in H; these facts are not obvious but they are straightforward to check.) Define $\psi\colon \mathbb{Z} \to H$ by $\psi(n) = \phi(n)$; so ψ is just ϕ, but with a different codomain. Then ψ is a bijective homomorphism from $\mathbb{Z}$ to H. This makes ψ an example of an *isomorphism*.

Isomorphisms are very special. If there is an isomorphism between two groups, we say they are *isomorphic* to each other. Most of the time, pairs of groups are not isomorphic to each other. Since $\mathbb{Z}$ and H are isomorphic, if we want to compute or solve equations in one of them, we can compute in the other one and move our inputs and answers back and forth using ψ and ψ^{-1}. In fact, every algebraic property of $\mathbb{Z}$ is also a property of H, since we can use ψ and ψ^{-1} to copy a proof about $\mathbb{Z}$ to a proof about H. For example, $+$ is commutative on $\mathbb{Z}$ and $\cdot$ is commutative on H (even though $\cdot$ is not commutative on $\mathrm{GL}_2(\mathbb{R})$).

Really, H is just $\mathbb{Z}$ written in code, and ϕ is the rule for encoding elements of $\mathbb{Z}$ as elements of H, and ϕ^{-1} is the rule for decoding them. It is not an overstatement to say that "being isomorphic" is the right notion of "being the same" in group theory. Really, in group theory, we are not studying the groups themselves, but rather the classes of isomorphic groups. It doesn't matter whether we are studying $\mathbb{Z}$ or this group H from the perspective of doing computations or solving equations.

2.3 The notion of subgroup

In the previous discussion, we introduced a group H. This H is a subset of $\mathrm{GL}_2(\mathbb{R})$, and the product operation on H is the same operation as the product on $\mathrm{GL}_2(\mathbb{R})$. This makes H a *subgroup* of $\mathrm{GL}_2(\mathbb{R})$. Since H was isomorphic to $\mathbb{Z}$, this makes H a copy of $\mathbb{Z}$ sitting inside of $\mathrm{GL}_2(\mathbb{R})$.

Most subsets of groups are not subgroups. For example, if $S = \{n^2 \in \mathbb{Z} | n \in \mathbb{Z}\}$, then S is not a subgroup of $\mathbb{Z}$, since usually sums of squares are usually not squares. The point is that $+$ does not define an operation on S, since $+$ the restriction of $+$ to S is a function $S \times S \to \mathbb{Z}$, but not a function $S \times S \to S$. So a requirement, for a subset even to have a chance to be a subgroup, is that the operation sends the subset into itself. This is called *closure*, and S is not closed under $+$.

Now consider $\mathbb{Z}_+$, the set of positive integers. Notice that $\mathbb{Z}_+$ is closed under $+$, since sums of positive integers are positive. So $+$ makes sense on $\mathbb{Z}_+$ as an operation. However, $\mathbb{Z}_+$ is still not a subgroup, because it is not a group under $+$. As we explained above, $\mathbb{Z}_+$ is not a group under $+$ because elements of $\mathbb{Z}_+$ do not have inverses.

A subset may be a group under a different operation, but it is not a subgroup unless it is a group under the same operation. For example $\mathbb{R}$ is a group under $+$, and the positive reals $\mathbb{R}_+$ is a group under multiplication $\cdot$, but $+$ does not restrict to $\cdot$, so it is not the same operation. Since $\mathbb{R}_+$ does not have additive inverses for its elements, it is not a group under $+$, and it is not a subgroup of $\mathbb{R}$.

The collection of subgroups of a group is an important part of the structure of that group. Subgroups have important connections to homomorphisms; for example, if H is a subgroup of G, then the inclusion map $i\colon H \to G$ defined by $i(x) = x$ is a homomorphism.

2.4 The notion of quotient groups

Quotient groups are perhaps the trickiest concept in basic group theory. Here is the motivating example. Fix a positive integer n. As we mentioned above, there is a set quotient $\mathbb{Z}/\sim$ of $\mathbb{Z}$, where $a \sim b$ means that a and b have the same remainder when divided by n. Write $\mathbb{Z}_n$ as notation for $\mathbb{Z}/\sim$. It is an interesting fact that if $a \sim b$, and $c \sim d$, then $a+c \sim b+d$. (Think about this.) This means that addition descends to an operation $+_n$ on $\mathbb{Z}_n$: for $[a]$ and $[c]$ in $\mathbb{Z}_n$, let $[a] +_n [c] = [a+c]$. This definition has a choice in it: if $a \sim b$, we could write $[a] = [b]$, so $[a] +_n [c] = [b] +_n [c] = [b+c]$. We need $[a+c] = [b+c]$ for this to be well defined. But this is true, since $a \sim b$ implies $a + c \sim b + c$. (A similar comment shows that it does not depend on the choice of representative of $[c]$.)

Then $\mathbb{Z}_n$ is a group that is a lot like $\mathbb{Z}$, except that $\mathbb{Z}_n$ has exactly n elements (and $\mathbb{Z}$ has infinitely many elements). Further, the function $p\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $p(a) = [a]$ is a homomorphism, and this means that there are structural connections between $\mathbb{Z}$ and $\mathbb{Z}_n$. Notice that this homomorphism is surjective but not injective.

Now let K be the set of integers divisible by n. It turns out that K is a subgroup of $\mathbb{Z}$ (it is a subset of $\mathbb{Z}$ that is a group under the same operation $+$). Notice that $a \sim b$ if and only if $-b + a \in K$. This lets us define $\sim$ in terms of K. This connection leads us to the usual notation for quotients: we write $\mathbb{Z}/K$ instead of writing $\mathbb{Z}/\sim$.

The intuition behind this example is that $\mathbb{Z}_n$ is the same as $\mathbb{Z}$, except that we have forgotten the integer quotient of dividing a by n, and remembered only the remainder. This forces us to consider integers to be the same if they have the same remainder modulo n. We have forgotten that these numbers are different, and yet this did not destroy all the algebraic structure. Instead $+$ descended into a simplified version of $+$.

However, there is a complication when taking quotients of groups that are not commutative. Consider the subgroup H of $\mathrm{GL}_2(\mathbb{R})$ we defined above. We can define an equivalence relation on $\mathrm{GL}_2(\mathbb{R})$ by saying $A \sim B$ if $B^{-1}A \in H$. However, this $\sim$ does not define a group quotient, because $\cdot$ does not descend to a well defined product on $\mathrm{GL}_2(\mathbb{R})/\sim$.

(Specifically, let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and let $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, and let I denote the 2×2 identity matrix. Then $A \sim I$ since $I^{-1} \cdot A = A \in H$, but $A \cdot B \not\sim I \cdot B$ since $B^{-1} \cdot A \cdot B \notin H$; you can check that $B^{-1} \cdot A \cdot B \notin H$. This means that $[A] \cdot [B]$ is not well defined in $\mathrm{GL}_2(\mathbb{R})/H$; it could be $[I \cdot B]$, using I as the representative of $[A]$, or it could be $[A \cdot B]$, using A as the representative of $[A]$, but $[I \cdot B] \neq [A \cdot B]$.)

To hint at how to overcome this difficulty, we show a different example. Recall that det is a function from $\mathrm{GL}_2(\mathbb{R})$ to $\mathbb{R}$ with the property that $\det(A \cdot B) = \det(A)\det(B)$. Define $N = \{A \in \mathrm{GL}_2(\mathbb{R}) | \det(A) = 1\}$. You can show that N is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. If $A \in N$, and $B \in \mathrm{GL}_2(\mathbb{R})$ (but B is not necessarily in N), it follows that $\det(B^{-1} \cdot A \cdot B) = \det(A) = 1$, so that

$B^{-1} \cdot A \cdot B \in N$. This makes N an example of a special kind of subgroup, called a *normal subgroup*. In particular, this makes $\mathrm{GL}_2(\mathbb{R})/N$ a well defined group. Define $\sim$ on $\mathrm{GL}_2(\mathbb{R})$ by making $A \sim B$ if $B^{-1} \cdot A \in N$. Then $A \sim B$ implies that $A \cdot C \sim B \cdot C$ and $C \cdot A \sim C \cdot B$ (follow your nose to prove this). This means that we can define $[A] \cdot [C] = [A \cdot C]$ and get a well defined product on $\mathrm{GL}_2(\mathbb{R})$. In fact, we get a group.

Intuitively, $\mathrm{GL}_2(\mathbb{R})/N$ is the same as $\mathrm{GL}_2(\mathbb{R})$, but we remember the determinants of matrices but forget the actual entries of the matrices. Since determinants of invertible matrices can be any nonzero real numbers, this means that $\mathrm{GL}_2(\mathbb{R})/N$ is isomorphic to $\mathbb{R}^\times$, the group of nonzero real numbers with multiplication as the operation.