LECTURE NOTES, WEEK 2

CHRIS KENNEDY

I'll make a disclaimer about these notes that holds for all future lecture notes as well: these may or may not be a good transcript of what happened in class. As a general rule, the lecture notes cover about 120% of what I hope to cover, but if we get sidetracked on something interesting, they may end up as only 80%. You never know. Hopefully, though, these will turn out to be useful.

1. Symmetries of a Square

As in problem set 0, consider a square with vertices going clockwise around, A, B, C, D. There are essentially eight things we can do to the square: rotate by 0, 90, 180, or 270 degrees; flip across the horizontal or vertical axis, or flip across the main diagonal or the off-main diagonal. In class, we called these $I, r_{90}, r_{90}^2, r_{90}^3, f_h, f_v, f_{AC}, f_{BD}$. For simplicity, I'm going to drop the 90 (so r is a rotation by $90°$). For reasons explained in a couple of pages, let's call this set D_4. Now, we notice a variety of things:

- If you compose two rotations, you get another one. For example, $r \cdot r^2 = r^3, r^3 \cdot r^2 = r, r^2 \cdot r^2 = I$, and so on. In particular, $r^4 = I$. Incidentally, we say that r has *order* 4, since 4 is the smallest positive power we can raise r to to get the identity. We'll have much more to say about order next time.
- Remembering that $f \cdot g$ means apply g first, then f (as in $(f \cdot g)(\square) = f(g(\square))$), we can compose other operations. So $f_v \cdot r = f_{AC}, r^3 \cdot f_h = f_{BD}$, and $f_{AC} \cdot f_{BD} = r^2$. Since composing any two symmetry operations gives us another one, we say they're *closed* under composition.
- We have an *identity* transformation, which leaves the square as is. If you apply the identity before or after some operation f, it's the same as just doing f itself; in other words, $I \cdot f = f \cdot I = f$ for any symmetry operation f.
- If you tediously compute, for example, $(f_v \cdot r) \cdot r^2$ and $f_v \cdot (r \cdot r^2)$, you find that, since $f_v \cdot r = f_{AC}$ and $r \cdot r^2 = r^3$, $(f_v \cdot r) \cdot r^2 = f_{BD} = f_v \cdot (r \cdot r^2)$. Since we just moved some parentheses around, we call this property *associativity*.
- Any operation has an inverse operation, one that brings the square back to its original position. For example, since $r \cdot r^3 = I$, r^3 is the inverse of r and vice versa. We say $r^{-1} = r^3$. By the same token, since any flip composed with itself is the identity, $f \cdot f = I$, or $f^2 = I$, meaning $f = f^{-1}$ for any flip f. Using the handy $\Rightarrow$ introduced in class (where $A \Rightarrow B$ means A implies B), we can write this as "f a flip $\Rightarrow f^2 = I \Rightarrow f = f^{-1}$".
- Finally, order matters! For example, $f_h \cdot r = f_{BD}$ but $r \cdot f_h = f_{AC}$. It's no coincidence, however, that changing the order still results in a flip across a diagonal–but this is a subtle point that we won't discuss until later.

We can collect all of these myriad observations in the following set of rules, using supercompact lazy notation (that is, using $\forall$ to mean "for all", $\exists$ to mean "there exists", and s.t. to mean "such that"):

Definition A *group* G is a set together with an operation $\cdot$ satisfying the following properties:

(1) (Closure) $\forall a, b \in G, a \cdot b \in G$.
(2) (Identity) $\exists I \in G$ s.t. $\forall a \in G, a \cdot I = I \cdot a = a$.
(3) (Associativity) $\forall a, b, c \in G, a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
(4) (Inverses) $\forall a \in G, \exists a^{-1} \in G$ s.t. $aa^{-1} = a^{-1}a = I$.

Date: Summer 2007.

If G satisfies a fifth property, that $a \cdot b = b \cdot a$ for all $a, b \in G$, then we say $\cdot$ is *commutative* and that G is a commutative group or *abelian* group. We'll return to all of this a bit later.

2. Things that look like the integers

We now head off in a somewhat different direction. Let's look at the set S of words made from the letters a and b, with the proviso that we remove any instance of ab or ba from S. So the words aaa and $bbbbb$ are fine, but $aaababba$ will be redacted to aa. If we use our knowledge of groups to try to understand S, we come up with the following:

- Any two words in S can be combined to give another one, assuming you redact enough. So aaa and $bbbbb$ can be shoved together as $aaabbbbb = bb$ or as $bbbbbaaa = bb$; it seems the operation of *concatenation* is closed and commutative in S. For the future, we can abbreviate things like $aaaa$ to a^4, just to make life easier.
- What is ab? We're supposed to eliminate it, leaving...nothing. We call this the *empty word*, or the identity. This makes sense–if you concatenate ab to the beginning or end of any word, it just gets redacted off. We can use the symbol e for ab (or ba, for that matter).
- Associativity holds; this isn't really all that interesting, so I'll leave it at that.
- What do we make of inverses? We know $ab = e$, so $a = b^{-1}$, and this generalizes pretty easily to $a^n = b^{-n}$ and $a^{-n} = b^n$. So everything has an inverse.

This means that, in short, S is a commutative group. The question is, what group is it? Well, you might notice that $a^n a^m = a^{n+m}$ and that $a^n b^m = a^{n-m}$. So multiplication in S looks like we're just messing with exponents. In fact, if we replace a with 1, b with -1, and concatenation with addition, everything is just happening in $\mathbb{Z}$, the integers. Just to get an idea for how this works, if we want to concatenate b^3 and a^7, we can either just do it in S, yielding $bbbaaaaaaa = aaaa = a^4$, or we could do it in $\mathbb{Z}$ by saying $b^3 = -3, a^7 = 7$, so $-3 + 7 = 4$, which becomes a^4, just as we had in S. This correspondence between S and $\mathbb{Z}$ is incredibly important (the idea of it, not specifically S), and is called an *isomorphism*. We say S is *isomorphic* to $\mathbb{Z}$, or $S \simeq \mathbb{Z}$.

To illustrate this concept with another example, let's look at the matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and its powers, collected in the set $T = \{A^n \text{ for all } n\}$. If we square A, for example, we get $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, and standard 2×2 matrix stuff tells us that $A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. This should be very suggestive already, especially when you throw in that $A^0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. In fact,

Proposition 2.1. *For all n, $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.*

Proof. We proceed by induction. For $n = 0$, this is trivial, as we have already established that $A^0 = I$. So assume $A^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$; we need to calculate A^{k+1}. This can be accomplished by multiplying by A again, so $A^k A = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$. Since the statement holds going from k to $k+1$, it holds for all n. □

Taking this a little further, a short computation shows $A^m A^n = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix} = A^{m+n}$, and this motivates us to say that T is isomorphic to $\mathbb{Z}$, just as S was. In particular, we set up a correspondence between $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ and n.

3. Basic Group Theory

It's time to get our hands dirty and actually work with groups somewhat abstractly. Since we've grown up a little since the first section, I'm going to drop the $\cdot$ unless it's really necessary to include. So first,

Theorem 3.1. *In a group G, the identity I is unique.*

Proof. Assume we had two identities, I and J. This means both of them satisfy the identity law for the group, that is, $Ia = aI = Ja = aJ = a$ for all a. But then $IJ = I$ since J is an identity, but also $IJ = J$ since I is an identity. Stringing these together, we get $I = J$, so the identity is unique. □

Using a similar idea, but a bit more mess, you can prove that the inverse of an element a is unique. As a quick exercise, convince yourself that $(a^{-1})^{-1} = a$ and that $(ab)^{-1} = b^{-1}a^{-1}$. Now let's look back briefly at our group D_4 from earlier. We noticed that the rotations seem to work nicely together–they are closed, have inverses, and are certainly associative. They are, in short, another group. This leads us to define

Definition If G is a group, then $H \subset G$ is a *subgroup* if H is itself a group.

So $\{1, r, r^2, r^3\}$ is a subgroup of D_4. We'll call it C_4. Some nice facts about subgroups:

Proposition 3.2. *If G is a group, then:*

1. *G and $\{e\}$ are subgroups. These are the trivial subgroups.*
2. *If H and K are subgroups of G, then so is $H \cap K$.*
3. *If H is a finite subset of G which is closed under $\cdot$, then H is a subgroup.*

Proof.

1. Since G is a group, it is clearly a subgroup, since $G \subset G$. As for $\{e\}$, it satisfies all the properties (since $ee = e, e^{-1} = e, e(ee) = (ee)e$), so it is also a subgroup.
2. Let $a, b \in H \cap K$. Then $ab \in H$ and $ab \in K$ since a, b are both in H and K, so $ab \in H \cap K$. Similarly $a^{-1} \in H \cap K$, and $e \in H \cap K$, all for the same reasons.
3. This one is a little trickier (but not tricky enough that I should have screwed it up–sorry about that). Let $a \in H$ be arbitrary. Then since H is closed, $a, a^2, a^3, \ldots$ must be in H as well. This is an infinite list, but H is finite, so two (well, many more, but for now we just need two) on that list must be the same. Say $a^m = a^n$ with $m > n$. Then $a^{m-n} = e$, so we have an identity. Furthermore, since $m > n, m - n > 0$ and so $m - n - 1 \geq 0$, meaning $a^{m-n-1} \in H$ (we have established that all nonnegative powers of a, including $a^0 = e$, are in H). But since $a^{m-n} = e, a^{m-n-1} = a^{m-n}a^{-1} = a^{-1}$, so $a^{-1} \in H$. We were given closure, we found an identity, we inherited associativity from G, and we found inverses, so H is a subgroup.

□

It's because of the third statement above that I hold that closure is the defining property of a group, and the one that requires the most cleverness to see (but usually not to prove). If you can find a closed operation on a set, you're almost certainly home free, because the other properties will almost always fall into place (not always! see the exercises).

4. Preview

Let's look ahead to next week just a bit. We've already defined cosets, and cosets are useful mainly for helping to prove some big theorems. The biggest one is Lagrange's theorem, which is stated below. In that statement, $o(H)$ means the number of elements in H, and $a \mid b$ should be taken to mean a divides b, or $b = ka$ for some integer k. So here's the statement:

Theorem 4.1. *(Lagrange) If H is a subgroup of G, then $o(H) \mid o(G)$.*

Proof. Next time! □

5. Exercises

Exercises are optional and for your own enjoyment. If you want to hand in solutions, I'll look at them, but that's by no means mandatory or expected. Exercises with a star (*) are harder. This week's exercises are a little tame, since I haven't really given you any big tools yet. So if these aren't that interesting, don't fret–next week's will have a juicier selection.

1. Can you find a group structure on sets? For operations, try union and/or intersection, and use whatever bunch of sets you want.

2. Prove that if $a^2 = 1$ for all a in some group G, then G is abelian.

3. Find all the subgroups of D_3.

4*. Prove that a cyclic group of prime order has no nontrivial subgroups (don't use Lagrange's theorem–this will give you a nice idea of how slippery things are without it!).

5. Find all the subgroups of D_p, where p is a prime number (Hint: use problem 4). If you're ambitious, prove you found all of them–this is a little trickier but not too bad.

6*. Prove that any two cosets of the same subgroup have the same number of elements (we'll do this next week).

7**. Prove Lagrange's theorem (Hint: use problem 6).

8*. Let S_3 be the group of permutations of 3 objects $\{a, b, c\}$. For example, one element of S_3 is swapping a and b, while another is cyclically permuting a to b, b to c, and c to a. Find the rest of the elements of S_3, and then prove it's isomorphic to D_3.