Lecture 19

Non-linear change of basis (group conjugation)

19.1 Goals

(1) Become familiar with the idea of conjugation (e.g., conjugating by an element g)

(2) Understand the notion of conjugacy class.

19.2 Group automorphisms

Definition 19.2.1. A function $f : G \to G$ is called a group *automorphism* if it is a group isomorphism. (So group automorphisms are special kinds of isomorphisms—those where the domain and codomain are the same group.)

We let

$$\mathrm{Aut}_{\mathrm{group}}(G)$$

denote the group of group automorphisms of G.

Remark 19.2.2. One should think of a group automorphism of G as a symmetry of the *group* G. This is a bit meta—G itself should be thought of as the symmetries of something, and $\mathrm{Aut}_{\mathrm{group}}(G)$ itself describes the symmetries of G.

Remark 19.2.3. Let h, h' be two elements of G. Suppose that there exists a group automorphism $f : G \to G$ for which $f(h) = h'$. Then—speaking

from the intuition that a group automorphism is a symmetry of G—any meaningful property that h has (as an element of the group G) must be shared by h'. (For example, we know that h and h' must have the same order.)

Let me make a geometric analogy to make this feel a bit closer to home. (Though we've only studied regular polygons in depth, make sure you try to imagine non-regular polygons in this paragraph.) Suppose P is some polygon. Suppose further that $f : P \to P$ is some symmetry of P and that $f(v) = v'$. Then v and v' must look very similar! For example, we immediately see that the angles at v and at v' must have the same measure. And there are more subtle ways in which v and v' must be similar—after all, given a polygon, just because two angles have the same angle measure, one cannot conclude that there is necessarily a symmetry of the whole polygon taking one angle to the other.

Likewise, if a group automorphism takes h to h', the two elements look very similar in ways far more subtle than just their orders.

Today, we're going to see a very special kind of group automorphism, given by *conjugaction*.

19.3 Conjugation and examples

Definition 19.3.1. Let G be a group, and g, h elements of G. Then the *conjugate of h by g* is the element ghg^{-1}.

Fixing g, one has a function $G \to G$ sending any h to the element ghg^{-1}. This function is called *conjugation by g*. We will call this function C_g.

Exercise 19.3.2. Let $G = S_3$, and let $\sigma = (13)$.

(a) What is σ^{-1}?

(b) What is the conjugate of $\tau = (12)$ by σ?

(c) What is the conjugate of $\tau = (132)$ by σ?

(d) Write out what the function C_σ does to every element of S_3.

Exercise 19.3.3. Let $G = S_3$, and let $\sigma = (123)$.

(a) What is σ^{-1}?

(b) Write out what the function C_σ does to every element of S_3.

19.4 Conjugation as a group automorphism

Conjugation is important for two distinct reasons. The first of these, as we will see now, is that group conjugation gives a symmetry of a group G itself.

Proposition 19.4.1. Let G be a group and fix $g \in G$. Then $C_g : G \to G$ is a group homomorphism (from G to itself).

Proof. Let h, h' be in G. Then

$$C_g(h)C_g(h') = (ghg^{-1})(gh'g^{-1}) = (gh)(g^{-1}g)(h'g^{-1}) = ghh'g^{-1} = g(hh')g^{-1} = C_g(hh').$$

The first equality is the definition of C_g (applied twice), the next equality is associativity, the next is the definition of g^{-1} (and of e), and the last equality is the definition of C_g again. □

Proposition 19.4.2. Let G be a group and $g \in G$.

(a) C_g is the inverse function to $C_{g^{-1}}$.

(b) C_g is a group automorphism.

Proof. For the first claim, we must simply show that for every $h \in G$, we have that

$$C_g(C_{g^{-1}}(h)) = h \qquad \text{and} \qquad C_{g^{-1}}(C_g(h)) = h.$$

To see the first equality, let's compute:

$$\begin{aligned} C_g(C_{g^{-1}}(h)) &= C_g(g^{-1}h(g^{-1})^{-1}) = C_g(g^{-1}hg) \\ &= g(g^{-1}hg)g^{-1} \\ &= (gg^{-1})h(gg^{-1}) \\ &= ehe \\ &= h. \end{aligned} \tag{19.4.0.1}$$

The first equality is by definition of $C_{g^{-1}}$, and the rest of the first line is by noting that the inverse of g^{-1} is g. The next lines follow from the definition of C_g, associativity, the definition of g^{-1}, and the definition of e, respectively.

The proof that $C_{g^{-1}}(C_g(h)) = h$ follows similarly.

Here is the proof of (b). We know that C_g is a group homomorphism by Proposition 19.4.1, and that it is a bijection by the proof of part (a). In other words, C_g is a group isomorphism. Of course C_g has both domain and codomain equal to G, so C_g is a group automorphism of G by definition of group automorphism (Definition 19.2.1). □

The following exercise tells us that group conjugation provides interesting symmetries only for non-abelian groups:

Exercise 19.4.3. Let G be an abelian group. Show that for any $g \in G$, the function C_g is the identity function of G.

The following tells us there are some group automorphisms that do not arise from conjugation:

Exercise 19.4.4. Show that $n \mapsto -n$ is a group automorphism of $\mathbb{Z}$ (under addition). Why is this automorphism not equal to conjugation by any element of $\mathbb{Z}$?

So, conjugation provides some special kinds of (i.e., not all) group automorphisms of a group G. This class of group automorphisms is trivial when G is abelian. Regardless, it is amazing that we can "automatically" write down symmetries of a group G without knowing anything about it! (For any $g \in G$, we are guaranteed that C_g is a group automorphism.) Because this class of automorphisms is so readily available (hence used often) we give it a name:

Definition 19.4.5. Let $f : G \to G$ be a group automorphism. We say that f is an *inner automorphism* if $f = C_g$ for some $g \in G$.

I will leave the following to you:

Proposition 19.4.6. The collection of inner automorphisms of G is a subgroup of $\mathrm{Aut}_{\mathrm{group}}(G)$.

The above proposition actually follows from:

Proposition 19.4.7. For any $g, g' \in G$, we have that $C_g C_{g'} = C_{gg'}$. In particular, the assignment $g \mapsto C_g$ is a group homomorphism

$$C_\bullet : G \to \mathrm{Aut}_{\mathrm{group}}(G).$$

Proof. Let's compute:

$$\begin{aligned}(C_g \circ C_{g'})(h) &= C_g(C_{g'}(h)) \\ &= C_g(g'h(g')^{-1}) \\ &= g(g'h(g')^{-1})g^{-1} \\ &= (gg')h((g')^{-1})g^{-1}) \\ &= (gg')h(gg')^{-1} \\ &= C_{gg'}(h).\end{aligned}$$

Make sure you can follow every line. We have used in particular that the inverse of gg' is the product $(g')^{-1}g^{-1}$. □

19.4.1 Conjugacy classes

The second reason we study conjugation is because, as we've discussed, conjugation tells us how "alike" two elements of a group G are. And, when a group G is finite, we can count how many elements look alike. This gives a powerful way to begin studying G, just as we can begin to study a polygon by understanding which of its vertices look alike.

Example 19.4.8. We saw in the previous section that inner automorphisms (i.e., conjugation) is a very special kind of automorphism, so if h and h' are in fact related by an inner automorphism, they are even more intimately indistinguishable.

This is so important that we give a name for when h is related to h' by an inner automorphism.

Definition 19.4.9. Let G be a group and $h, h' \in G$. We say that h *is conjugate to* h' if there exists some $g \in G$ for which $ghg^{-1} = h'$.

Exercise 19.4.10. Show that "being conjugate" is an equivalence relation.

Definition 19.4.11. The equivalence class of h, under conjugation, is called the *conjugacy class of* h. We often write the conjugacy class of h as $Cl(h)$. Concretely,

$$Cl(h) = \{h' \text{ such that, for some } g \in G,\ h' = ghg^{-1}\}.$$

Equivalently,

$$Cl(h) = \{ghg^{-1} \mid g \in G\}.$$

Remark 19.4.12. So the way to write down the conjugacy class of some element h is to take *every* $g \in G$ and write out the conjugates ghg^{-1}.

Remark 19.4.13. Again using the intuition that elements taken to each other under inner automorphisms are very similar, the conjugacy class $Cl(h)$ is a list of all the elements in G that share all the group-theoretic properties that h satisfies as an element of G. In other words, it is a list of elements that are as similar to h as you can get.

Exercise 19.4.14. Let $G = S_3$.

(a) Write out the conjugacy class of (12). (The conjugacy class should consist of three elements.)

(b) At this point, why is it easy to write out the conjugacy class of (23)?

(c) Let's test our intuition that conjugate elements are alike: In what ways are the elements in your conjugacy class alike?

(d) Write out the conjugacy class of (123). (The conjugacy class should consist of two elements.)

(e) At this point, why is it easy to write out the conjugacy class of (132)?

(f) Let's test our intuition that conjugate elements are alike: In what ways are the elements in the two classes you've computed *not* alike. That is, are there obvious ways in which an element $h \in Cl((23))$ is unlike an element $h' \in Cl((123))$?

Exercise 19.4.15. Let G be abelian, and choose any $h \in G$. Show that $Cl(h)$ contains exactly one element.

19.5 Conjugacy classes of the symmetric group

It turns out that cycle notation is also amazing for understanding conjugacy classes of the symmetric group.

Theorem 19.5.1. Fix $n \geq 1$. Two elements of S_n are conjugate if and only if they have the same cycle notation shape.

Example 19.5.2. For example, the element

$$\sigma = (13)(56)(7982)$$

and the element

$$\tau = (59)(24)(1386)$$

are clearly different elements of S_9, but their cycle notations have the same shape—consisting of two 2-cycles and one 4-cycle. The theorem tells us they are conjugate.

It is in fact easy to write down the element g that conjugates them. Note that to "turn σ into τ" one can make the substitutions

$$1 \mapsto 5, \qquad 2 \mapsto 6, \qquad 3 \mapsto 9, \qquad 4 \mapsto 7, \qquad 5 \mapsto 2,$$

$$6 \mapsto 4, \qquad 7 \mapsto 1, \qquad 8 \mapsto 8, \qquad 9 \mapsto 3.$$

This substitution is itself an element of S_9, which we'll call h. Then one can check that conjugation by h turns σ to τ.

Once you internalize the theorem, you don't have to do any computations of function-composition to do the following exercise:

Exercise 19.5.3. (a) Write out all the conjugacy classes of S_4. (This is a bit annoying because S_4 has 24 elements.)

(b) How many conjugacy classes are there?

(c) How many elements are in the conjugacy classes you found?

19.6 Some exercise solutions

Solution to Exercise 19.3.2. (a) σ is its own inverse. Indeed, $(13)\circ(13) = ()$. One way to think of this intuitively is that σ is a function which does nothing to 2, and swaps 1 and 3. If I swap two elements, and I perform the same swap, of course I end up with the same configuration I began with.

(b) Let's do this out carefully. The conjugate of τ by σ is, by definition: $\sigma\tau\sigma^{-1}$. Plugging in the permutations that these symbols stand for, we find:

$$\sigma\tau\sigma^{-1} = (13)(12)(13) = (13)(132) = (23).$$

So the conjugate of τ by σ is (23). You could have also written this as (32). Notice that (32) is exactly the cycle you would obtain from τ by replacing every instance of 1 by 3, and every instance of 3 by 1 (as σ prescribes).

(c) When $\tau = (132)$, we compute:

$$\sigma\tau\sigma^{-1} = (13)(132)(13) = (13)(12) = (123).$$

You could also have written (123) as the equivalent cycle (312). Notice that (312) is exactly what one obtains from $\tau = (132)$ by swapping every instance of 1 by 3, and of 3 by 1 (just as σ prescribes).

(d) We have so far seen that

$$C_\sigma((12)) = (23) \qquad \text{and} \qquad C_\sigma((132)) = (123).$$

We have four more elements of S_3 to compute C_σ for. They are $e = (), (23), (123)$ and (13) (σ itself). Let's compute:

$$C_\sigma(e) = \sigma e \sigma^{-1} = \sigma\sigma^{-1} = e.$$

$$C_\sigma((23)) = (13)(23)(13) = (13)(123) = (12).$$
$$C_\sigma((123)) = (13)(123)(13) = (13)(23) = (132).$$
$$C_\sigma((13)) = \sigma\sigma\sigma^{-1} = \sigma = (13).$$

In short, C_σ acts as follows:

$$\begin{aligned} e &\mapsto e \\ (12) &\mapsto (23) \\ (23) &\mapsto (12) \\ (13) &\mapsto (13) \\ (132) &\mapsto (123) \\ (123) &\mapsto (132). \end{aligned}$$

By the way, one fun thing to check is that C_σ squares to the identity function. In other words, $C_\sigma \circ C_\sigma = \mathrm{id}_{S_3}$. One way to see this without computing C_σ is to note that $C_\sigma \circ C_\tau = C_{\sigma\tau}$ in general, so $C_\sigma \circ C_\sigma = C_{\sigma\sigma} = C_e = \mathrm{id}$.

□