II.G. Conjugacy and the orbit-stabilizer theorem

II.G.1. PROPOSITION. *Let $g \in G$. Mapping $h \mapsto ghg^{-1}$ defines an isomorphism $\imath_g \colon G \to G$.*

PROOF. HW. [Hint: use II.E.6(ii).] □

II.G.2. DEFINITION. (i) $\imath_g$ is called **conjugation by g**.
(ii) $g', g'' \in G$ are said to be **conjugate** if there is a $g \in G$ such that $g'' = \imath_g(g')$.
(iii) $H', H'' \leq G$ are said to be conjugate if there is a $g \in G$ such that $H'' = \imath_g(H')$.

II.G.3. PROPOSITION. (i) *Conjugate groups are isomorphic.*
(ii) *Conjugate elements are of the same order.*

PROOF. The restriction of $\imath_g$ gives the isomorphism in (i), and (ii) follows from (i) by taking $H' = \langle g' \rangle$, $H'' = \langle g'' \rangle$. □

Now consider the *action of G on itself by conjugation*

$$g.g_0 := gg_0g^{-1}. \tag{II.G.4}$$

The orbits of this action are called the **conjugacy classes** of G. There are two notational ambiguities to get rid of here: first, since G can act on itself in more than one way, we don't write $G(g)$; second, if an element lies in a subgroup $H \leq G$, we need to distinguish G- and H-orbits. (Even if the G-orbit lies in H, the H-orbit can be smaller.)

II.G.5. DEFINITION. Let $g_0 \in G$. The **conjugacy class of $\mathbf{g_0}$ in G** is

$$\mathrm{ccl}_G(g_0) := \{gg_0g^{-1} \mid g \in G\}.$$

The conjugacy class of $1 \in G$ is always just the singleton $\{1\}$.

II.G.6. PROPOSITION. *G is abelian if and only if all of its conjugacy classes have one element.*

PROOF. $gh = hg$ $(\forall g, h \in G) \iff ghg^{-1} = h$ $(\forall g, h \in G) \iff \mathrm{ccl}_G(h) = \{h\}$ $(\forall h \in G)$. □

So let's find the conjugacy classes in a couple of groups.

II.G.7. EXAMPLE. Let's consider $G = \mathfrak{S}_3$. We know that $\mathrm{ccl}_{\mathfrak{S}_3}(1) = \{1\}$. Computing, one finds that

$$\begin{aligned}\mathrm{ccl}_{\mathfrak{S}_3}((12)) = \{&1(12)1^{-1},\ (12)(12)(12)^{-1};\ (13)(12)(13)^{-1},\\ &(123)(12)(123)^{-1};\ (132)(12)(132)^{-1},\ (23)(12)(23)^{-1}\}\\ &= \{(12);\ (23);\ (13)\}\\ &= \mathrm{ccl}_{\mathfrak{S}_3}((13)) = \mathrm{ccl}_{\mathfrak{S}_3}((23)),\end{aligned}$$

consists of all the transpositions, while

$$\begin{aligned}\mathrm{ccl}_{\mathfrak{S}_3}((123)) &= \{(12)(123)(12)^{-1}, \ldots\}\\ &= \{(132),\ (123)\} = \mathrm{ccl}_{\mathfrak{S}_3}((132))\end{aligned}$$

contains both 3-cycles.

Now, rather than using brute force, we could cut down our work by noticing that elements of $\mathrm{ccl}_{\mathfrak{S}_3}((12))$ *must* (like (12)) have order 2, hence be transpositions. But there is a still more powerful result.

II.G.8. DEFINITION. The **cycle-structure** of a permutation $\sigma \in \mathfrak{S}_n$ is the sequence

$$\begin{cases} b_1 = & \text{\# of fixed elements} \\ b_2 = & \text{\# of transpositions} \\ b_3 = & \text{\# of 3-cycles} \\ & \vdots \\ b_n = & \text{\# of } n\text{-cycles} \end{cases}$$

in σ's complete factorization into disjoint cycles. (More commonly, we represent it symbolically, viz. $(\cdot\cdot)(\cdot\cdot)(\cdot\cdot\cdot)(\cdot)$.)

II.G.9. THEOREM. $\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)$ *consists of all permutations with the same cycle-structure as* σ.

PROOF. Write $\sigma = (a_{11}a_{12}\cdots a_{1d_1})\cdots(a_{k1}a_{k2}\cdots a_{kd_k})$ as a product of disjoint cycles (of lengths $d_1, \ldots, d_k$), with each element of

$\{1, \ldots, n\}$ appearing exactly once. For each $\eta \in \mathfrak{S}_n$, we have

$$\begin{aligned}\eta\sigma\eta^{-1} &= \eta(a_{11}a_{12}\cdots a_{1d_1})\eta^{-1}\cdots\eta(a_{k1}a_{k2}\cdots a_{kd_k})\eta^{-1}\\ &= (\eta(a_{11})\eta(a_{12})\cdots\eta(a_{1d_1}))\cdots(\eta(a_{k1})\eta(a_{k2})\cdots\eta(a_{kd_k}))\end{aligned}$$

by your last HW. That is, we just apply η to all the "contents", which preserves the disjointness (η is bijective) and the lengths of the cycles, hence the cycle structure. Finally, given *any* permutation with the same cycle structure as σ

$$\sigma' = (b_{11}b_{12}\cdots b_{1d_1})\cdots(b_{k1}\cdots b_{kd_k})$$

then taking

$$\eta := \begin{pmatrix} a_{11}a_{12}\cdots a_{kd_k} \\ b_{11}b_{12}\cdots b_{kd_k}\end{pmatrix},$$

we have $\sigma' = \eta\sigma\eta^{-1}$. □

II.G.10. EXAMPLE. Consider $G = D_5$. Recall that $rh = hr^{-1}$ (and $h = h^{-1}$, and $r^{-1} = r^4$); that is,

$$\begin{aligned} rhr^{-1} = rrh = r^2h &\implies r^a h r^{-a} = r^{2a}h \\ hrh^{-1} = r^{-1}hh^{-1} = r^{-1} &\implies hr^a h^{-1} = r^{-a}. \end{aligned}$$

So $\mathrm{ccl}_{D_5}(h) = \{h, r^2h, r^4h, r^6h = rh, r^8h = r^3h\} = \mathrm{ccl}_{D_5}(r^2h) = \cdots$ and $\mathrm{ccl}_{D_5}(r) = \{r, r^4\}$, $\mathrm{ccl}_{D_5}(r^2) = \{r^2, r^3\}$, $\mathrm{ccl}_{D_5}(1) = \{1\}$. In a picture,

$$\boxed{h \quad rh \quad r^2h \quad r^3h \quad r^4h}$$
$$\boxed{1} \quad \boxed{r \quad r^4} \quad \boxed{r^2 \quad r^3}$$

displays the four conjugacy classes in D_5.

The conjugacy classes in the last two examples partition G into disjoint subsets. This is true in general:

$$x \sim y \quad \iff \quad \exists\, g \in G \text{ s.t. } y = gxg^{-1}$$
$$(x \text{ and } y \text{ are conjugate})$$

defines an equivalence relation on G. The equivalence classes are the conjugacy classes; and if we take one representative g_i of each, then (by I.A.5) we have

$$G = \coprod_i \mathrm{ccl}(g_i). \qquad \text{(II.G.11)}$$

More generally, if G acts on a set X and we define[12]

$$\begin{aligned} x \sim y \quad &\underset{\text{def.}}{\iff} \quad y \in G(x) \\ &\iff \quad \boxed{x, y \text{ in same } G\text{-orbit}} \ (*) \end{aligned}$$

then

<u>$\sim$ is reflexive</u>: $x \in G(x) \implies x \sim x$
<u>$\sim$ is symmetric</u>: clear from $(*)$
<u>$\sim$ is transitive</u>: $y = g.x$ and $z = h.y \implies z = h.(g.x) = hg.x$.

hence defines an equivalence relation. Of course, $\mathrm{X}/\sim$ is the set of orbits $G(x)$, which by I.A.5 are disjoint with union all of X. If $|\mathrm{X}| < \infty$, and we pick one element x_i in each orbit, then

$$\mathrm{X} = \coprod_i G(x_i). \qquad \text{(II.G.12)}$$

Now we turn to our first counting result — a sort of analogue of Lagrange's Theorem for group actions.

II.G.13. EXAMPLE. First let's look at the sizes of orbits and stabilizers in the actions by conjugation from our last two examples:

(i) <u>orbit</u>: $\mathrm{ccl}_{\mathfrak{S}_3}((12)) = \{(12), (23), (13)\}$ (3 elements)
<u>stabilizer</u>: $(\mathfrak{S}_3)_{(12)} = \{1, (12)\}$ (2 elements)
... and $|\mathfrak{S}_3| = 6 = 3 \cdot 2$.

(ii) <u>orbit</u>: $\mathrm{ccl}_{D_5}(h) = \{h, rh, r^2h, r^3h, r^4h\}$ (5 elements)
<u>stabilizer</u>: $(D_5)_h = \{1, h\}$ (2 elements)
... and $|D_5| = 10 = 5 \cdot 2$.

It appears we are on to something. In the (big) statement that follows, G/G_x will denote the set of left cosets of G_x in G.

[12] To see the second "$\iff$" below: the forward implication is trivial, since $x \in G(x)$ too. Conversely, suppose x, y are in the same G-orbit $G(z)$, viz. $x = g.z$ and $y = h.z$. Then $hg^{-1}.x = hg^{-1}g.z = h.z = y$, so $y \in G(x)$.

II.G.14. THEOREM. *Let $x \in X$ be fixed.*
(i) *There is a 1-to-1 correspondence between points in the orbit of x and cosets of its stabilizer — that is, a bijective map of sets:*

$$G(x) \stackrel{(\dagger)}{\longrightarrow} G/G_x$$
$$g.x \longmapsto gG_x.$$

(ii) **[Orbit-Stabilizer Theorem]** *If $|G| < \infty$, then*

$$\boxed{|G(x)| \cdot |G_x| = |G|.}$$

(iii) *If x, x' belong to the same orbit, then G_x and $G_{x'}$ are conjugate as subgroups of G (hence of the same order/etc.).*
(iv) *If g, g' belong to the same (left) coset of G_x, then they act the same way on x.*

PROOF. (i) We have $g.x = g'.x \iff x = g^{-1}g'.x \iff g^{-1}g' \in G_x \iff g^{-1}g'G_x = G_x \iff gG_x = g'G_x$, which proves ($\dagger$) is well-defined and injective. Surjectivity is obvious.
(ii) LHS($\dagger$) has size $|G(x)|$; while RHS($\dagger$) has size $|G/G_x| =$ # of cosets of G_x, which by Lagrange's Theorem is $|G|/|G_x|$.
(iii) The calculation is: if $x' = g.x$, then $h \in G_x \iff h.x = x \iff gh.x = g.x \iff ghg^{-1}.(g.x) = g.x \iff ghg^{-1} \in G_{x'}$. So $G_{x'} = \imath_g(G_x)$.
(iv) is pretty much a direct verbal translation of (i). $\square$

We want to apply II.G.14 to compute conjugacy classes. Recall once more that in a group G, acting on itself by conjugation (and $x \in G$), the orbit

$$G(x) = \{gxg^{-1} \mid g \in G\} =: \mathrm{ccl}_G(x)$$

is called the *conjugacy class of x*; while the stabilizer

$$G_x = \{g \in G \mid gxg^{-1} = x\} = C_G(x)$$

is called the *centralizer of* x. The Orbit-Stabilizer Theorem then says that

$$|\text{ccl}_G(x)| \cdot |C_G(x)| = |G|. \tag{II.G.15}$$

Next recall (Theorem II.G.9) that *for* $\sigma \in \mathfrak{S}_n$, $\text{ccl}_{\mathfrak{S}_n}(\sigma)$ *consists of all permutations with the same cycle-structure as* σ. Since it is already the cycle-structure which determines whether an element is in $\mathfrak{A}_n$, it follows that

$$\text{if } \sigma \in \mathfrak{A}_n, \text{ then } \text{ccl}_{\mathfrak{S}_n}(\sigma) \subset \mathfrak{A}_n. \tag{II.G.16}$$

Here is a counting result for conjugacy classes in $\mathfrak{S}_n$.

II.G.17. PROPOSITION. *The number of permutations in* $\mathfrak{S}_n$ *with cycle-structure* $b_1, b_2, \ldots, b_n$ (*cf. II.G.8*) *is*

$$\frac{n!}{\prod_{k=1}^n k^{b_k} b_k!}.$$

PROOF. First, lay out the "chambers" into which you are going to insert the elements $\{1, \ldots, n\}$ to get a cycle:

$$\underbrace{(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)}_{b_2=3}\ \underbrace{(\cdot\cdot\cdot)}_{b_3=1}\ \underbrace{(\cdot\cdot\cdot\cdot)(\cdot\cdot\cdot\cdot)}_{b_4=2}\ \text{ etc.}$$

Choose an ordering of $\{1, \ldots, n\}$ (there are $n!$ possibilities) and plop them down in that order. Now divide by the cyclic permutations *within* each chamber (there are $\prod_{k=1}^n k^{b_k} = 2^{b_2}3^{b_3}4^{b_4}\cdots$ of these). Finally, divide out by permutations *of* chambers of the same length (there are $\prod_{k=1}^n b_k!$ of these). □

Before going on, you should reconceptualize this proof as an application of (II.G.15).

II.G.18. EXAMPLES. (i) $|\text{ccl}_{\mathfrak{S}_6}((12)(34)(56))| = \frac{6!}{2\cdot 2\cdot 2\cdot 3!} = 15$.
(ii) $|\text{ccl}_{\mathfrak{S}_6}((12345)(6))| = \frac{6!}{(5\cdot 1!)(1\cdot 1!)} = 144$.
(iii) $|\text{ccl}_{\mathfrak{S}_6}(1234)(56))| = \frac{6!}{(4\cdot 1!)(2\cdot 1!)} = 90$.
The order of the centralizer is, in each case, $\frac{6!}{|\text{ccl}_{\mathfrak{S}_6}(\cdots)|}$.

Now in spite of II.G.16, we may not have $\mathrm{ccl}_{\mathfrak{S}_n}(\sigma) = \mathrm{ccl}_{\mathfrak{A}_n}(\sigma)$ for $\sigma \in \mathfrak{A}_n$:

II.G.19. THEOREM. *Given $\sigma \in \mathfrak{A}_n$, one has* EITHER

(I) $|\mathrm{ccl}_{\mathfrak{A}_n}(\sigma)| = |\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)| \underset{equiv.}{\iff} C_{\mathfrak{S}_n}(\sigma)$ *contains an odd permutation*

OR

$$\text{(II)} \quad |\mathrm{ccl}_{\mathfrak{A}_n}(\sigma)| = \tfrac{1}{2}|\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)| \underset{equiv.}{\iff} C_{\mathfrak{S}_n}(\sigma) \subset \mathfrak{A}_n.$$

In the second case, one says that the conjugacy class "breaks" in $\mathfrak{A}_n$.

PROOF. By (II.G.15) (applied twice),

$$\text{(II.G.20)} \quad |\mathrm{ccl}_{\mathfrak{A}_n}(\sigma)||C_{\mathfrak{A}_n}(\sigma)| = |\mathfrak{A}_n| = \tfrac{1}{2}|\mathfrak{S}_n| = \tfrac{1}{2}|\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)||C_{\mathfrak{S}_n}(\sigma)|.$$

If $C_{\mathfrak{S}_n}(\sigma) \subset \mathfrak{A}_n$, then $C_{\mathfrak{A}_n}(\sigma) = C_{\mathfrak{S}_n}(\sigma)$ and so by (II.G.20) $|\mathrm{ccl}_{\mathfrak{A}_n}(\sigma)| = \frac{1}{2}|\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)|$.

Otherwise, $C_{\mathfrak{S}_n}(\sigma)$ contains an element of $\mathfrak{S}_n \backslash \mathfrak{A}_n$ (the odd permutations), and $C_{\mathfrak{A}_n}(\sigma) < C_{\mathfrak{S}_n}(\sigma)$, which by Lagrange means that

$$\frac{|C_{\mathfrak{S}_n}(\sigma)|}{|C_{\mathfrak{A}_n}(\sigma)|} \geq 2.$$

But by (II.G.20) $\mathrm{ccl}_{\mathfrak{A}_n}(\sigma) \subseteq \mathrm{ccl}_{\mathfrak{S}_n}(\sigma) \implies |\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)||C_{\mathfrak{A}_n}(\sigma)| \geq \frac{1}{2}|\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)||C_{\mathfrak{S}_n}(\sigma)| \implies$

$$\frac{|C_{\mathfrak{S}_n}(\sigma)|}{|C_{\mathfrak{A}_n}(\sigma)|} \leq 2$$

(hence $= 2$). It follows that $|\mathrm{ccl}_{\mathfrak{S}_n}(\sigma)| = |\mathrm{ccl}_{\mathfrak{A}_n}(\sigma)|$. □

II.G.21. EXAMPLES. (i) All 3-cycles are conjugate in $\mathfrak{A}_5$: since "all 3-cycles" is a conjugacy class (of some σ, say (123)) in $\mathfrak{S}_5$, we are claiming $\mathrm{ccl}_{\mathfrak{S}_5}((123)) = \mathrm{ccl}_{\mathfrak{A}_5}((123))$. By II.G.19, it is enough to show that $C_{\mathfrak{S}_5}((123))$ contains an odd permutation — i.e., that (123) *commutes with* an odd permutation; and (45) does the job.

(ii) All 3-cycles are *not* conjugate in $\mathfrak{A}_4$: that is, $\mathrm{ccl}_{\mathfrak{A}_4}((123))$ is not all the 3-cycles ($= \mathrm{ccl}_{\mathfrak{S}_4}((123))$), and we are in case (II) of II.G.19. To check this, we need to compute $C_{\mathfrak{S}_4}((123))$: what permutations η satisfy $\eta(123)\eta^{-1} (= (\eta(1)\eta(2)\eta(3))) = (123)$? Clearly just the cyclic group $\langle(123)\rangle$, which is indeed in $\mathfrak{A}_4 \underset{II.G.19}{\Longrightarrow} |\mathrm{ccl}_{\mathfrak{A}_4}((123))| = \frac{1}{2}|\mathrm{ccl}_{\mathfrak{S}_4}((123))|$.

(iii) How about $\mathrm{ccl}_{\mathfrak{A}_8}(\overbrace{(123)(4567)}^{\sigma})$ and $\mathrm{ccl}_{\mathfrak{A}_8}(\overbrace{(123)(45678)}^{\eta})$?

- σ commutes with an odd permutation, namely (4567), and so σ has the same conjugacy classes in $\mathfrak{A}_8$ and $\mathfrak{S}_8$.
- η commutes with only elements of the group $\langle(123),(45678)\rangle$ which consists of even permutations. So $|\mathrm{ccl}_{\mathfrak{A}_8}(\eta)| = \frac{1}{2}|\mathrm{ccl}_{\mathfrak{S}_8}(\eta)|$.

We mention in passing the conjugacy classes of a couple of other groups: for D_{2n+1} (odd dihedral group) they are

$$\{1\},\ \{r,r^{-1}\},\ \{r^2,r^{-2}\},\ldots,\{r^n,r^{-n}\};\ \ \{h,rh,r^2h,\ldots,r^{2n}h\}$$

and for D_{2n} (even dihedral group)

$$\{1\},\ \{r,r^{-1}\},\ \{r^2,r^{-2}\},\ \ldots,\ \{r^{n-1},r^{-n+1}\},\ \{r^n\};$$
$$\{h,r^2h,r^4h,\ldots,r^{2n-2}h\},\ \{rh,r^3h,\ldots,r^{2n-1}h\}.$$

These are obtained by repeatedly applying $rh = hr^{-1}$ as in II.G.10.

There is also Hamilton's famous **quaternion** group:

II.G.22. DEFINITION. $Q := \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$, with $\mathbf{ijk} = \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$.

The conjugacy classes are $\{1\},\ \{-1\},\ \{\mathbf{i},-\mathbf{i}\},\ \{\mathbf{j},-\mathbf{j}\},\ \{\mathbf{k},-\mathbf{k}\}$. For example, $\mathbf{jij}^{-1} = -\mathbf{jij} = \mathbf{jij}(\mathbf{kk}) = \mathbf{j}(\mathbf{ijk})\mathbf{k} = -\mathbf{jk} = \mathbf{iijk} = -\mathbf{i}$.

II.G.23. REMARK. Hamilton arrived at the multiplication table for Q by "formally dividing vectors in $\mathbb{R}^3$", allowing himself

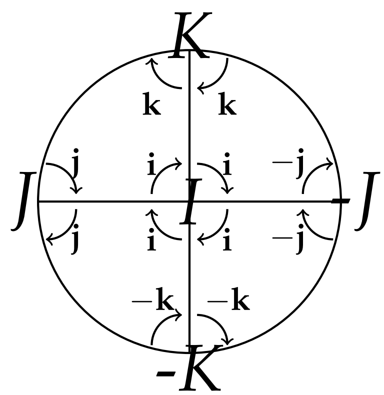
$$\frac{\alpha\vec{x}}{\beta\vec{x}} = \frac{\alpha}{\beta},\quad \frac{\vec{x}}{\vec{y}}\cdot\frac{\vec{y}}{\vec{z}} = \frac{\vec{x}}{\vec{z}},\quad \text{and}\quad \frac{\vec{x}}{\vec{y}} = \frac{R_\theta(\vec{x})}{R_\theta(\vec{y})}$$

for any rotation R_θ in the plane spanned by $\vec{x}$ and $\vec{y}$. One is also supposed to think "$\frac{\vec{x}}{\vec{y}}\cdot\vec{y} = \vec{x}$", but *don't* try to think too literally in terms of linear transformations!

Taking I, J, K to be the standard basis of $\mathbb{R}^3$, one can write (using 90° rotations[13] about I, J, and K respectively)

$$\mathbf{i} := \tfrac{K}{J} = \tfrac{-J}{K}, \quad \mathbf{j} := \tfrac{I}{K} = \tfrac{-K}{I}, \quad \mathbf{k} := \tfrac{J}{I} = \tfrac{-I}{J},$$

which Hamilton encoded in a diagram:



Furthermore, we have $\mathbf{i}^2 = \frac{-J}{K} \cdot \frac{K}{J} = \frac{-J}{J} = -1$, $\mathbf{ij} = \frac{J}{-K} \cdot \frac{-K}{I} = \frac{J}{I} = \mathbf{k}$, $\mathbf{ji} = \frac{I}{K} \cdot \frac{K}{J} = \frac{I}{J} = -\mathbf{k} = -\mathbf{ij}$, and $\mathbf{ijk} = \frac{-J}{K} \cdot \frac{-K}{I} \cdot \frac{-I}{J} = -1$, and so on.

Now, to be honest, there are problems with the idea of "dividing vectors in $\mathbb{R}^3$", since at the end of the day there can be no "3-dimensional division algebra over $\mathbb{R}$" (as we'll see later this semester). In any case, we get the right nonabelian group of order 8 and that's all we care about presently!

[13]One is supposed to think of $\mathbf{i}$ as "counterclockwise rotation around I" and so on.