21. Permutation groups II

21.1. **Conjugacy classes.** Let G be a group, and consider the following relation $\sim$ on G: given $f, h \in G$, we put

$$f \sim h \iff \text{there exists } g \in G \text{ s.t. } h = gfg^{-1}.$$

Thus, in the terminolgy from Lecture 20, $f \sim h \iff h$ is a conjugate of f.

Definition. The relation $\sim$ is called the conjugacy relation.

Lemma 21.0. *The conjugacy relation $\sim$ is an equivalence relation on G.*

Proof. (i) Reflexivity: for every $f \in G$ we have $efe^{-1} = f$, so $f \sim f$ (that is, f is a conjugate of itself).

(ii) Symmetry: assume that $f \sim h$, so that $h = gfg^{-1}$ for some $g \in G$. Then $f = g^{-1}hg = uhu^{-1}$ where $u = g^{-1} \in G$. Therefore, $h \sim f$.

(iii) Transitivity: assume that $f \sim h$ and $h \sim k$, so that $h = g_1 f g_1^{-1}$ and $k = g_2 h g_2^{-1}$ for some $g_1, g_2 \in G$. Then $k = g_2 g_1 f g_1^{-1} g_2^{-1} = gfg^{-1}$ where $g = g_2 g_1 \in G$, so $f \sim k$. □

Having established that $\sim$ is symmetric, we can safely use the terminology "f and h are conjugate" instead of saying "h is a conjugate of f."

Definition. The equivalence classes with respect to the conjugacy relation are called the conjugacy classes of G. For each $f \in G$ we denote its conjugacy class by $K(f)$. Thus,

$$K(f) = \{h \in G : h = gfg^{-1} \text{ for some } g \in G\}.$$

Note that by the general properties of equivalence classes, conjugacy classes form a partition of G, that is, distinct conjugacy classes are disjoint, and the union of all conjugacy classes of G is the entire group G.

Warning: Conjugacy classes should not be confused with cosets.

21.2. **Conjugacy classes in S_n.** Computation of conjugacy classes in a given group may be a complicated problem. However, conjugacy classes in permutation groups admit a very simple and explicit description.

We start with an example showing how conjugation works in S_n.

Example: Let $n \geq 3$, let $f = (1,2,3) \in S_n$, and let g be some element of S_n. Let us compute the conjugate $gfg^{-1} = g(1,2,3)g^{-1}$.

To do this we have to track the image of each $i \in \{1,\ldots,n\}$ under the composed map. First we analyze where gfg^{-1} sends $g(1)$, $g(2)$ and $g(3)$. We have

$$\begin{aligned} g(1) &\xrightarrow{g^{-1}} 1 \xrightarrow{f} 2 \xrightarrow{g} g(2) \\ g(2) &\xrightarrow{g^{-1}} 2 \xrightarrow{f} 3 \xrightarrow{g} g(3) \\ g(3) &\xrightarrow{g^{-1}} 3 \xrightarrow{f} 1 \xrightarrow{g} g(1). \end{aligned}$$

Now take any $i \neq g(1), g(2)$ or $g(3)$. Then (since g is bijective) we have $g^{-1}(i) \neq 1, 2$ or 3, and therefore $f(g^{-1}(i)) = g^{-1}(i)$. Thus we get

$$i \xrightarrow{g^{-1}} g^{-1}(i) \xrightarrow{f} g^{-1}(i) \xrightarrow{g} i.$$

So, gfg^{-1} maps $g(1)$ to $g(2)$, $g(2)$ to $g(3)$, $g(3)$ to $g(1)$, and fixes all other elements. Therefore, $gfg^{-1} = g(1,2,3)g^{-1} = (g(1), g(2), g(3))$.

It is not hard to see that similar formula is true in general: for any cycle $(i_1,\ldots,i_k)$ and any $g \in S_n$ we have

$$g(i_1,\ldots,i_k)g^{-1} = (g(i_1),\ldots,g(i_k)). \tag{K1}$$

In other words, if f is a cycle of length k, then gfg^{-1} is also a cycle of length k whose entries are obtained by applying g to the entries of f.
If f is a product of several cycles, the conjugate gfg^{-1} is obtained by applying the same procedure to each cycle in the decomposition of f. This is true because of the following formula:

$$\text{if } f = f_1 f_2 \ldots f_t, \text{ then } gfg^{-1} = (gf_1g^{-1})(gf_2g^{-1})\ldots(gf_tg^{-1}). \tag{K2}$$

Theorem 21.1. *Let $f, h \in S_n$. Then f and h are conjugate in S_n if and only if f and h have the same cycle type.*

Proof. Formulas (K1) and (K2) immediately imply that for any $g \in G$, the elements f and gfg^{-1} have the same cycle type. This proves the "⇒" direction.

"⇐" We need to show that if f and h have the same cycle type, then there exists $g \in G$ such that $h = gfg^{-1}$. The general proof involves somewhat messy notations, so instead we illustrate it in a special case.

Let us take $n = 7$, $f = (1,2,3)(4,5)$ and $h = (1,3,5)(2,7)$. By (K1) and (K2) for any $g \in S_7$ we have $gfg^{-1} = (g(1), g(2), g(3))(g(4), g(5))$. Clearly, to have the equality $gfg^{-1} = h$ we can take any $g \in S_7$ such that

$$g(1) = 1, \quad g(2) = 3, \quad g(3) = 5, \quad g(4) = 2, \quad g(5) = 7. \tag{$***$}$$

The only other restriction is that g is bijective. We have to decide what $g(6)$ and $g(7)$ are. We have two "unused outputs", 4 and 6, so we can set $g(6) = 4$ and $g(7) = 6$, or $g(6) = 6$ and $g(7) = 4$ (both choices work). The main point is that such g exists.

Remark: The condition (***) was sufficient, but not necessary to have the equality $gfg^{-1} = h$. For instance, since $(1,3,5) = (3,5,1)$, we could let $g(1) = 3$, $g(2) = 5$ and $g(3) = 1$ (keeping the remaining values of g unchanged) and still have the desired equality.

The algorithm for finding g which conjugates f into h can be made even more direct. Let us write f and h in cycle form, including fixed points, and put the expression for h right below the expression for f:

$$f = (1,2,3)(4,5)(6)(7)$$
$$h = (1,3,5)(2,7)(4)(6)$$

Then the element g, which sends each integer in the first line to the integer in the second line right below it, has the desired property $h = gfg^{-1}$ (in our example we get $g(1) = 1$, $g(2) = 3$, $g(3) = 5$, $g(4) = 2$, $g(5) = 7$, $g(6) = 4$ and $g(7) = 6$). Since both lines contain every integer from 1 to 7 precisely once, such g is bijective.

This alternative description clearly shows that the algorithm described in this example can be applied to any two elements f and h of the same cycle type. □

As an immediate consequence of Theorem 21.1 we obtain an explicit description of conjugacy classes in S_n:

Corollary 21.2. *For every $f \in S_n$, its conjugacy class $K(f)$ consists of all elements in S_n which have the same cycle type as f.*

Example: Describe conjugacy classes in S_4:

cycle type	an element of that type f	the conjugacy class $K(f)$	$\lvert K(f)\rvert$
$1+1+1+1$	e	e	1
$2+1+1$	$(1,2)$	$(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$	6
$2+2$	$(1,2)(3,4)$	$(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$	3
$3+1$	$(1,2,3)$	$(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$ $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$	8
4	$(1,2,3,4)$	$(1,2,3,4)$, $(1,2,4,3)$, $(1,3,2,4)$ $(1,3,4,2)$, $(1,4,2,3)$, $(1,4,3,2)$	6

Note that $1+6+3+8+6 = 24 = |S_4|$, as should be the case since conjugacy classes of a group G form a partition of G.

21.3. **Normal subgroups in S_n.** Recall the statement of Theorem 20.2 (conjugation criterion of normality): Let G be a group and H a subgroup of G. Then

$$H \text{ is normal in } G \iff \text{for every } h \in H \text{ and } g \in G \text{ we have } ghg^{-1} \in H.$$

In other words, H is normal in $G \iff$ for every $h \in H$, all conjugates of h (by elements of G) lie in H.

Having introduced the notion of a conjugacy class, we can now state a useful reformulation of this theorem.

Theorem 21.3. *Let G be a group and H a subgroup of G. Then H is normal in $G \iff$ for every conjugacy class $K(x)$ in G, either $K(x) \subseteq H$ or $K(x) \cap H = \emptyset$. In other words,*

$$H \textit{ is normal in } G \iff H \textit{ is a union of (some) conjugacy classes of } G.$$

Proof. Let us prove the forward direction ("$\Rightarrow$"); the backward direction is analogous. So, assume that H is normal in G. We need to show that if $x \in G$ is such that $K(x) \cap H \neq \emptyset$, then $K(x) \subseteq H$.

If $K(x) \cap H \neq \emptyset$, then there exists $h \in K(x) \cap H$, and thus $K(h) \cap K(x) \neq \emptyset$ (since $h \in K(h)$), that is, the conjugacy classes of h and x overlap. But any two conjugacy classes in G are either disjoint or coincide, so we must have $K(x) = K(h)$. By definition, $K(h) = \{y \in G : y = ghg^{-1} \text{ for some } g \in G\}$. Since $h \in H$ and H is normal, Theorem 20.2 implies that $K(h) \subseteq H$, and therefore $K(x) = K(h) \subseteq H$, which is what wanted to prove. □

Warning: Theorem 21.3 does NOT say that a union of conjugacy classes is always a normal subgroup. This is because a union of conjugacy classes may not be a subgroup at all. What it says is that if a union of conjugacy classes is a subgroup, then this subgroup is normal, and moreover, all normal subgroups can be obtained in this way.

Example: Find all normal subgroups in $G = S_4$.
We found earlier that S_4 has 5 conjugacy classes K_1, K_2, K_3, K_4, K_5 whose sizes are $n_1 = |K_1| = 1$, $n_2 = |K_2| = 3$, $n_3 = |K_3| = 6$, $n_4 = |K_4| = 8$ and $n_5 = |K_5| = 6$. Now let H be a normal subgroup of S_4. Then by Theorem 21.3, H is the union of some the $K_i' s$, so $|H|$ is the sum of some of the n_i's (since distinct conjugacy classes are disjoint). Moreover,

(i) $n_1 = 1$ must be included since H must contain e (and $e \in K_1$);
(ii) the sum of the n_i's we use (which is equal to $|H|$) must divide $24 = |S_4|$ by Lagrange theorem.

Below we consider all possible collections of n_i's which include n_1 and eliminate those which do not satisfy conidition (ii) (that is, where the sum is not a divisor of 24).

collection	sum	candidate?
1	1	yes
1,3	1+3=4	yes
1,6	1+6=7	no
1,8	1+8=9	no
1,3,6	1+3+6=10	no
1,3,8	1+3+8=12	yes

It is easy to see that in all other collections of n_i's, the sum will be > 12, so the only way we can get a divisor of 24 is if the sum is equal to 24 (which means that we used all n_i's).

Summarizing, any normal subgroup H must be equal to one of the following.

(1) $H = K_1$, in which case $|H| = n_1 = 1$
(2) $H = K_1 \cup K_2$, in which case $|H| = n_1 + n_2 = 1 + 3 = 4$
(3) $H = K_1 \cup K_2 \cup K_4$, in which case $|H| = n_1 + n_2 + n_4 = 1 + 3 + 8 = 12$
(4) $H = \cup_{i=1}^5 K_i$, in which case $|H| = \sum_{i=1}^5 n_i = 24$.

As explained above, each of the sets (1)-(4) is either a normal subgroup or not a subgroup at all, so we only need to check whether these sets are subgroups.

In case (1) we have $H = \{e\}$ (which is a subgroup), and in case (4) $H = G = S_4$ (which is also a subgroup). Of course, we could say right away that $\{e\}$ and G are normal subgroups of G – this would be true in any group.

In case (2) we have $H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. This is a subgroup by direct verificaiton. It is sometimes denoted by V_4 and called the Klein four group. It is a group of order 4 isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

In case (3) we have

$$H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3), (1,3,2), (1,2,4), (1,4,2), \\ (1,3,4), (1,4,3), (2,3,4), (2,4,3)\}.$$

In this case we note that H consists precisely of all even permutations in S_4, so $H = A_4$ is a subgroup.

So, the final answer is that S_4 has 4 normal subgroups: $\{e\}, V_4, A_4$ and S_4. Note that the more interesting part of the argument was not showing that these subgroups are normal, but showing that there are no other normal subgroups.

Also note that in this example we did not get any unions of conjugacy classes which are not subgroups but which cannot be eliminated by conditions (i)-(ii) above. This is pretty rare, and usually there will be some "false positives" which will have to be eliminated later.

Homework tip. In Problem 8 of Homework#10 you are asked to solve the corresponding problem for S_5. Since S_5 is much larger than S_4, explicitly listing all permutations in each conjugacy classes is no longer a good option; instead you should find a way to count the number of permutations in each conjugacy class (equivalently, the number of permutations of each cycle type). Here we illustrate how to do this for two cycles types in S_5.

Let us start with 5-cycles (that is, cycles of length 5). A naive guess is that there should be $5! = 120$ such cycles – this, however, is easily seen to be wrong since 120 is the total number of permutations in S_5, and not all of them are 5-cycles. The reason 120 is not the right answer is that we can shift the integers cyclically within the cycle without changing the permutation. Note that if $(i_1, i_2, i_3, i_4, i_5) \in S_5$ is a 5-cycle, then each integer from 1 to 5 must appear in it, so after a cyclic shift we can assume that the cycle starts with 1, that is, $i_1 = 1$. After that we have 4 choices for i_2, 3 choices for i_3 etc.; in total $4! = 24$ choices. It is also clear that any two 5-cycles starting with 1 represent the same element of S_5 if and only if they are identical. So, our 24 choices yield 24 distinct elements in S_5. Summarizing, we found that the number of 5-cycles in S_5 is 24.

Next we turn to cycle type $4 + 1$ (a 4-cycle and a fixed point). Here we have 5 choices to decide which element will be the fixed point and, once the fixed point has been chosen, $3! = 6$ ways to choose the 4-cycle (by the same logic is above). In total we get that there are $5 \cdot 6 = 30$ elements in the cycle type $4 + 1$.

Enumeration of elements in other cycle types is similar (though not completely analogous). Special care should be taken with cycle type $2+2$ (product of two disjoint transpositions) – do you see why?