21 Symmetric and alternating groups

Recall. The symmetric group on n letters is the group

$$S_n = \mathrm{Perm}(\{1, \dots, n\})$$

21.1 Theorem (Cayley). *If G is a group of order n then G is isomorphic to a subgroup of S_n.*

Proof. Let S be the set of all elements of G. Consider the action of G on S

$$G \times S \to S, \quad a \cdot b := ab$$

This action defines a homomorphism $\varrho\colon G \to \mathrm{Perm}(S)$. Check: this homomorphism is 1-1. It follows that G is isomorphic to a subgroup of $\mathrm{Perm}(S)$. Finally, since $|S| = n$ we have $\mathrm{Perm}(S) \cong S_n$. $\square$

21.2 Notation. Denote

$$[n] := \{1, \dots, n\}$$

If $\sigma \in S_n$, $\sigma\colon [n] \to [n]$ then we write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

21.3 Definition. A permutation $\sigma \in S_n$ is a *cycle of length* r (or r*-cycle*) if there are distinct integers $i_1, \dots, i_r \in [n]$ such that

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \dots\ ,\ \sigma(i_r) = i_1$$

and $\sigma(j) = j$ for $j \neq i_1, \dots, i_r$.

A cycle of length 2 is called a *transposition*.

Note. The only cycle of length 1 is the identity element in S_n.

21.4 Notation. If σ is a cycle as above then we write

$$\sigma = (i_1\ i_2\ \ldots\ i_r)$$

21.5 Example. In S_5 we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} = (2\ 4\ 5\ 3)$$

Note: $(2\ 4\ 5\ 3) = (4\ 5\ 3\ 2) = (5\ 3\ 2\ 4) = (3\ 2\ 4\ 5)$.

21.6 Definition. Permutations $\sigma, \tau \in S_n$ are *disjoint* if

$$\{i \in [n] \mid \sigma(i) \neq i\} \ \cap \ \{j \in [n] \mid \tau(j) \neq j\} = \varnothing$$

21.7 Proposition. *If σ, τ are disjoint permutations then $\sigma\tau = \tau\sigma$.*

Proof. Exercise. $\square$

21.8 Proposition. *Every non-identity permutation $\sigma \in S_n$ is a product of disjoint cycles of length ≥ 2. Moreover, this decomposition into cycles is unique up to the order of factors.*

21.9 Example. Let $\sigma \in S_9$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 1 & 3 & 2 & 6 & 5 & 9 & 8 \end{pmatrix}$$

Then $\sigma = (1\ 4\ 3)(2\ 7\ 5)(8\ 9)$.

Proof of proposition 21.8. Consider the action of $\mathbb{Z}$ on the set $[n]$ given by

$$k \cdot i = \sigma^k(i)$$

for $k \in \mathbb{Z}$, $i \in [n]$. Notice that

$$\mathrm{Orb}(i) = \{\sigma^k(i) \ \mid \ k \in \mathbb{Z}\}$$

Define $\sigma_i \colon [n] \to [n]$

$$\sigma_i(j) = \begin{cases} \sigma(j) & \text{if } j \in \mathrm{Orb}(i) \\ j & \text{otherwise} \end{cases}$$

Notice that σ_i is a bijection since $\sigma(\mathrm{Orb}(i)) = \mathrm{Orb}(i)$. Thus $\sigma_i \in S_n$. Check:

1) σ_i is a cycle of length $|\mathrm{Orb}(i)|$.
2) if $\mathrm{Orb}(i_1), \dots, \mathrm{Orb}(i_r)$ are all distinct orbits of $[n]$ containing more than one element then $\sigma_{i_1}, \dots, \sigma_{i_r}$ are non-trivial, disjoint cycles and

$$\sigma = \sigma_{i_1} \cdot \ldots \cdot \sigma_{i_r}$$

Uniqueness of decomposition - easy. □

21.10 Proposition. *Every permutation $\sigma \in S_n$ is a product of (not necessarily disjoint) transpositions.*

Proof. By Proposition 21.8 it is enough to show that every cycle is a product of transpositions. We have:

$$(i_1 \ i_2 \ i_3 \ \dots \ i_r) = (i_1 \ i_r)(i_1 \ i_{r-1}) \cdot \ldots \cdot (i_1 \ i_3)(i_1 \ i_2)$$

□

Note. For $\sigma \in S_n$ we have a bijection

$$\sigma \times \sigma \colon [n] \times [n] \to [n] \times [n]$$

given by $\sigma \times \sigma(i,j) = (\sigma(i), \sigma(j))$. Define

$$S_\sigma := \{(i,j) \in [n] \times [n] \mid i > j \text{ and } \sigma(i) < \sigma(j)\}$$

21.11 Definition. A permutation $\sigma \in S_n$ is *even* (resp. *odd*) if the number of elements of S_σ is even (resp. odd).

21.12 Theorem. *1) The map* $\operatorname{sgn}\colon S_n \to \mathbb{Z}/2\mathbb{Z}$ *defined by*

$$\operatorname{sgn}(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd} \end{cases}$$

is a homomorphism.

2) If σ is a transposition then $\operatorname{sgn}(\sigma) = 1$, *so this homomorphism is non-trivial.*

Proof. 1) Let $\sigma, \tau \in S_n$. Denote $s_\sigma = |S_\sigma|$. We want to show

$$s_{\tau\sigma} \equiv s_\tau + s_\sigma \pmod 2$$

Let $[n]^+ := \{(i,j) \in [n] \times [n] \mid i > j\}$. Define subsets $P_\sigma, R_\sigma, P_\tau, R_\tau \subseteq [n]^+$ as follows:

$$\begin{aligned} P_\sigma &:= \{(i,j) \mid \sigma^{-1}(i) > \sigma^{-1}(j)\} \\ R_\sigma &:= \{(i,j) \mid \sigma^{-1}(i) < \sigma^{-1}(j)\} \\ P_\tau &:= \{(i,j) \mid \tau(i) > \tau(j)\} \\ R_\tau &:= \{(i,j) \mid \tau(i) < \tau(j)\} \end{aligned}$$

Notice that $s_\sigma = |R_\sigma|$ and $s_\tau = |R_\tau|$. Notice also that $(i,j) \in S_{\tau\sigma}$ iff either $(\tau(i), \tau(j)) \in P_\sigma \cap R_\tau$ or $(\tau(j), \tau(i)) \in R_\sigma \cap P_\tau$. This gives

$$s_{\tau\sigma} = |P_\sigma \cap R_\tau| + |R_\sigma \cap P_\tau|$$

On the other hand we have:

$$s_\sigma = |R_\sigma| = |R_\sigma \cap P_\tau| + |R_\sigma \cap R_\tau|$$

$$s_\tau = |R_\tau| = |P_\sigma \cap R_\tau| + |R_\sigma \cap R_\tau|$$

Therefore

$$s_\sigma + s_\tau = |R_\sigma \cap P_\tau| + |P_\sigma \cap R_\tau| + 2|R_\sigma \cap R_\tau| = s_{\tau\sigma} + 2|R_\sigma \cap R_\tau|$$

and so $s_\tau + s_\sigma \equiv s_{\tau\sigma} \pmod 2$.

2) Exercise. $\square$

21.13 Definition/Proposition. The set

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$$

is a normal subgroup of S_n. It is called the *alternating group on n letters*.

Proof. It is enough to notice that $A_n = \mathrm{Ker}(\mathrm{sgn})$. $\square$

Note. We have

$$S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$$

Since $|S_n| = n!$ thus $|A_n| = \frac{n!}{2}$.

21.14 Proposition. *If $\sigma \in S_n$ then σ is even (resp. odd) iff σ is a product of an even (resp. odd) number of transpositions.*

Proof. If $\sigma = \tau_1 \ldots \tau_m$ where $\tau_1, \ldots, \tau_m$ are transpositions then

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1 \ldots \tau_m) = \sum_{i=1}^{m} \operatorname{sgn}(\tau_i) = \sum_{i=1}^{m} 1$$

Thus $\operatorname{sgn}(\sigma) = 0$ iff m is even and $\operatorname{sgn}(\sigma) = 1$ iff m is odd.

□

Note. If follows that if a permutation $\sigma \in S_n$ is a product of an even number of transpositions then it cannot be written as a product of an odd number of transpositions (and vice versa).

21.15 Corollary. *A permutation $\sigma \in S_n$ is even iff*

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_r$$

where σ_i is a cycle of length m_i and $\sum_{i=1}^{r}(m_r + 1)$ is even.

Proof. It is enough to notice that by the proof of Proposition 21.10 a cycle of length m is a product of $m + 1$ transpositions. □

Note. The usual notation for the sign of a permutation is

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

where $\{-1, 1\} \cong \mathbb{Z}/2\mathbb{Z}$ is the multiplicative group of units in $\mathbb{Z}$.

22 Simplicity of alternating groups

22.1 Theorem. *The alternating group A_n is simple for $n \geq 5$.*

22.2 Lemma. *For $n \geq 3$ every element of A_n is a product of 3-cycles.*

Proof. It is enough to show that if $n \geq 3$ and τ, σ are transpositions in S_n then $\tau\sigma$ is a product of 3-cycles.

Case 1) τ, σ are disjoint transpositions: $\tau = (i\ j)$, $\sigma = (k\ l)$ for distinct elements $i, j, k, l \in [n]$. Then we have

$$\tau\sigma = (i\ j\ k)(j\ k\ l)$$

Case 2) τ, σ are not disjoined: $\tau = (i\ j)$, $\sigma = (j\ k)$. Then

$$\tau\sigma = (i\ j\ k)$$

□

22.3 Lemma. *If $n \geq 5$ and σ, σ' are 3-cycles in S_n then*

$$\sigma' = \tau\sigma\tau^{-1}$$

for some $\tau \in A_n$

Proof. Check: if $(i_1\ i_2\ \ldots\ i_r)$ is a cycle in S_n then for any $\omega \in S_n$ we have

$$\omega(i_1\ i_2\ \ldots\ i_r)\omega^{-1} = (\omega(i_1)\ \omega(i_2)\ \ldots \omega(\ i_r))$$

If $\sigma = (i_1\ i_2\ i_3)$, $\sigma' = (j_1\ j_2\ j_3)$ then take $\omega \in S_n$ such that $\omega(i_k) = j_k$ for $k = 1, 2, 3$. We have

$$\sigma' = \omega\sigma\omega^{-1}$$

If $\omega \in A_n$ we can then take $\tau := \omega$.

Assume then that $\omega \notin A_n$. Since $n \geq 5$ there are $r, s \in [n]$ such that $(r\ s)$ and $\sigma = (i_1\ i_2\ i_3)$ are disjoint cycles. Take $\tau = \omega(r\ s)$. Then $\tau \in A_n$. Moreover, since $(r\ s)$ commutes with σ we have

$$\tau\sigma\tau^{-1} = \omega(r\ s)\sigma(r\ s)^{-1}\omega^{-1} = \omega\sigma\omega^{-1} = \sigma'$$

□

22.4 Corollary. *If $n \geq 5$ and H is a normal subgroup of A_n such that H contains some 3-cycle then $H = A_n$.*

Proof. By Lemma 22.3 H contains all 3-cycles, and so by Lemma 22.2 it contains all elements of A_n. □

Proof of Theorem 22.1. Let $n \geq 5$, $H \lhd A_n$ and $H \neq \{(1)\}$. We need to show that $H = A_n$. By Corollary 22.4 it will suffice to show that H contains some 3-cycle.

Let $(1) \neq \sigma$ be an element of H with the maximal number of fixed points in $[n]$. We will show that σ is 3-cycle. Take the decompositon of σ into dosjoint cycles:

$$\sigma = \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_m$$

Case 1) $\sigma_1, \ldots, \sigma_m$ are transpositions.

Since $\sigma \in A_n$ we must then have $m \geq 2$. Say, $\sigma_1 = (i\ j)$, $\sigma_2 = (k\ l)$. Take $s \neq i, j, k, l$ and let $\tau = (k\ l\ s) \in A_n$. Since H is normal in A_n we have

$$\tau\sigma\tau^{-1}\sigma^{-1} \in H$$

Check:

1) $\tau\sigma\tau^{-1}\sigma^{-1} \neq (1)$ since $\tau\sigma\tau^{-1}\sigma^{-1}(k) \neq k$

2) $\tau\sigma\tau^{-1}\sigma^{-1}$ fixes every element of $[n]$ fixed by σ

3) $\tau\sigma\tau^{-1}\sigma^{-1}$ fixes i, j.

Thus $\tau\sigma\tau^{-1}\sigma^{-1}$ has more fixed points than σ which is impossible by the definition of σ.

Case 2) σ_r is a cycle of length ≥ 3 for some $1 \leq r \leq m$.

We can assume $r = 1$: $\sigma_1 = (i\ j\ k \ldots)$. If $\sigma = \sigma_1$ and σ_1 is a 3-cycle we are done.

Otherwise σ must move at least two more elements, say p, q. In such case take $\tau = (k\ p\ q)$. We have

$$\tau\sigma\tau^{-1}\sigma^{-1} \in H$$

Check:

1) $\tau\sigma\tau^{-1}\sigma^{-1} \neq (1)$ since $\tau\sigma\tau^{-1}\sigma^{-1}(k) \neq k$

2) $\tau\sigma\tau^{-1}\sigma^{-1}$ fixes every element of $[n]$ fixed by σ

3) $\tau\sigma\tau^{-1}\sigma^{-1}$ fixes j.

Thus $\tau\sigma\tau^{-1}\sigma^{-1}$ has more fixed points than σ which is again impossible by the definition of σ.

As a consequence σ must be a 3-cycle.

$\square$

22.5. Classification of simple finite groups.

1) cyclic groups $\mathbb{Z}/p\mathbb{Z}$, p – prime

2) alternating groups A_n, $n \geq 5$

3) finite simple groups of Lie type, e.g. projective special linear groups

$$PSL_n(\mathbb{F}) := SL_n(\mathbb{F})/Z(SL_n(\mathbb{F}))$$

$\mathbb{F}$ -finite field, $n \geq 2$ (and $n > 2$ if $\mathbb{F} = \mathbb{F}_2$ or $\mathbb{F} = \mathbb{F}_3$).

4) 26 sporadic groups (the smallest: Mathieu group M_{11}, $|M_{11}| = 7920$, the biggest: the Monster M, $|M| \approx 8 \cdot 10^{53}$).

23 Solvable groups

Recall. Every finite group G has a composition series:

$$\{e\} = G_0 \subseteq \ldots \subseteq G_k = G$$

where $G_{i-1} \lhd G_i$ and G_i/G_{i-1} is a simple group.

23.1 Definition. A group G is *solvable* if it has a composition series

$$\{e\} = G_0 \subseteq \ldots \subseteq G_k = G$$

such that for every i the group G_i/G_{i-1} is a simple abelian group (i.e. $G_i/G_{i-1} \cong \mathbb{Z}/p_i\mathbb{Z}$ for some prime p_i).

23.2 Example.

1) Every finite abelian group is solvable.

2) For $n \geq 5$ the symmetric group S_n has a composition series

$$\{(1)\} \subseteq A_n \subseteq S_n$$

and so S_n is not solvable.

23.3 Proposition. *A finite group G is solvable iff it has a normal series*

$$\{e\} = H_0 \subseteq \ldots \subseteq H_l = G$$

such that H_j/H_{j-1} is an abelian group for all j.

Proof. Exercise. $\square$

Recall.

1) If G is a group the $[G,G]$ is the commutator subgroup of G

$$[G,G] = \langle\{aba^{-1}b^{-1} \ \mid \ a,b \in G\}\rangle$$

2) $[G,G]$ is the smallest normal subgroup of G such that $G/[G,G]$ is abelian: if G/H for some $H \lhd G$ then $[G,G] \subseteq H$.

23.4 Definition. For a group G the *derived series of* G is the normal series

$$\cdots \subseteq G^{(2)} \subseteq G^{(1)} \subseteq G^{(0)} = G$$

where $G^{i+1} = [G^{(i)}, G^{(i)}]$ for $i \geq 1$. The group $G^{(i)}$ is called the *i-th derived group of G.*

23.5 Theorem. *A group G is solvable iff $G^{(n)} = \{e\}$ for some $n \geq 0$.*

Proof. Exercise. □

23.6 Theorem.

1) *Every subgroup of a solvable group is solvable.*
2) *Ever quotient group of a solvable group is solvable.*
3) *If $H \lhd G$, and both H and G/H are solvable groups then G is also solvable.*

Proof.

1) If $H \subseteq G$ then $H^{(i)} \subseteq G^{(i)}$. Thus if $G^{(n)} = \{e\}$ then $H^{(n)} = \{e\}$.

2) For $H \lhd G$ take the canonical epimorphism $f\colon G \to G/H$. We have

$$f(G^{(i)}) = (G/H)^{(i)}$$

Therefore if $G^{(n)} = \{e\}$ then $(G/H)^{(n)} = \{e\}$.

3) Assume that $H \lhd G$, and that $H^{(m)}$, $(G/H)^{(n)}$ are trivial groups. Consider the canonical epimorphism $f\colon G \to G/H$. We have

$$f(G^{(n)}) = (G/H)^{(n)} = \{e\}$$

Therefore $G^{(n)} \subseteq \mathrm{Ker}(f) = H$. As a consequence we obtain

$$G^{(n+m)} = \left(G^{(n)}\right)^{(m)} \subseteq H^{(m)} = \{e\}$$

□

23.7 Theorem (Feit-Thompson)**.** *Every finite group of odd order is solvable.*

Proof. See:
W. Feit, J.G. Thompson, *Solvability of groups of odd order*, Pacific Journal of Mathematics 13(3) (1963), 775-1029. □

23.8 Corollary. *There are no non-abelian finite simple groups of odd order.*

Proof. Let $G \neq \{e\}$ be a simple group of odd order. By Theorem 23.7 G is solvable so $[G, G] \neq G$. Since $[G, G] \lhd G$, by simplicity of G we must have $[G, G] = \{e\}$, and so G is an abelian group. □