NOTATION. Let X be a set with n elements, e.g. $X=\{1,\dots,n\}$.
The <u>symmetric group</u> S_X is the group of all permutations of X, i.e. bijections $\pi: X\to X$, with composition of maps as multiplication. For $X=\{1,\dots,n\}$, S_X is denoted by S_n.
For each finite sequence of distinct elements $x_1,\dots,x_\ell\in X$, the permutation $\gamma\in S_X$ with

$$\gamma(x_1)=x_2,\ \gamma(x_2)=x_3,\dots,\gamma(x_\ell)=x_1 \quad\text{and}\quad \gamma(x)=x \text{ for } x\notin\{x_1,\dots,x_\ell\}$$

is a <u>cycle</u> or an <u>ℓ-cycle</u>; we write $\gamma=(x_1,\dots,x_\ell)$ or simply $\gamma=(x_1\cdots x_\ell)$.
Each 1-cycle (x) fixes every element in X and is usually written 1. Within a cycle, the elements may be permuted cyclically, e.g. $(12)=(21)$ & $(123)=(231)=(312)$

THM A For each finite set X, each $\pi\in S_X$ is a product of disjoint cycles, corresponding to the orbits of $\langle\pi\rangle$ in its action on X.

Proof. Let A be an orbit of $\langle\pi\rangle$ on X. Let $x_1\in A$. Put *)

$x_2=\pi x_1,\ x_3=\pi x_2,\dots$ until the first repetition, say $x_{\ell+1}=x_m$ for some $m\le\ell$.
If $m>1$, then $x_\ell=\pi^{-1}x_{\ell+1}=\pi^{-1}x_m=x_{m-1}$, so there is an earlier repetition, contradiction. So $m=1$, so $A=\{x_1,\dots,x_\ell\}$ and the action of $\langle\pi\rangle$ on A is a cycle $(x_1\cdots x_\ell)$.
Since X is a disjoint union of $\langle\pi\rangle$-orbits, we see that π is a a product of the corresponding (disjoint) cycles. (In this product, the factors may be written in any order, since disjoint cycles commute, e.g. $(12)(345)=(345)(12)$.)

LEMMA F. If $\pi\in S_X$ has the disjoint cycle decomposition

$$\pi=(x_1\cdots x_{\ell_1})(y_1\cdots y_{\ell_2})\cdots,$$

then for each $\lambda\in S_X$,

$$(\pi^\lambda=)\ \lambda\pi\lambda^{-1}=(\lambda(x_1)\cdots\lambda(x_{\ell_1}))(\lambda(y_1)\cdots\lambda(y_{\ell_2}))\cdots.$$

*) For simplicity we sometimes drop the parentheses, writing πx_1 instead of $\pi(x_1)$.

Proof What does $\lambda\pi\lambda^{-1}$ do to $\lambda(x_1)$?

$$(\lambda\pi\lambda^{-1})(\lambda(x_1)) = \lambda(\pi(\lambda^{-1}(\lambda(x_1)))) = \lambda(\pi(x_1)) = \lambda(x_2).$$

Similarly for $\lambda(x_2), \cdots$, i.e.

$$(\lambda\pi\lambda^{-1})(\lambda(x_1)) = \lambda(x_2), \cdots, \lambda\pi\lambda^{-1}(\lambda(x_\ell)) = \lambda(x_1),$$

so $(\lambda(x_1), \cdots, \lambda(x_\ell))$ is a cycle in the permutation $\lambda\pi\lambda^{-1}$. Similarly for the other cycles in π and corresponding cycles in $\lambda\pi\lambda^{-1}$.

NOTATION. Let $\pi \in S_X$ with $|X| = n$. Because the cycles in a disjoint cycle factorization $\checkmark$ of π commute, we may write them in any order, e.g. in order of decreasing length, giving

$$\boxed{n = \ell_1 + \ell_2 + \cdots \quad \text{with } \ell_1 \geq \ell_2 \geq \cdots > 0},$$

a <u>partition of n</u>. The partition $\square$ is called the <u>cycle</u> type of π.

THM B Let X be a finite set, $n = |X|$. Two elements π & $\pi' \in S_X$ are conjugate $\iff$ they have the same cycle structure, so the number $k(S_X)$ of conjugacy classes in S_X equals the number of partitions $\square$ of n.

Proof. By lemma 1, if π' and π are conjugate, i.e. $\pi' = \pi^\lambda$, for some $\lambda \in S_X$, then π' and π have the same cycle type. Conversely, if π' and π in S_X have the same cycle type, i.e. besides $\checkmark$ we have

$$\checkmark' \quad \pi' = (x_1' \cdots x_{\ell_1}')(y_1' \cdots y_{\ell_2}') \cdots \quad ,$$

then the permutation λ sending

$$x_i \text{ to } x_i' \text{ for } 1 \leq i \leq \ell_1, \quad y_j \text{ to } y_j' \text{ for } 1 \leq j \leq \ell_2, \cdots$$

satisfies $\pi^\lambda = \pi'$, by Lemma 1, showing that π' is conjugate to π.

EXAMPLE The symmetric group S_4 has five conjugacy classes, corresponding to the five partitions $4, 3+1, 2+2, 2+1+1, 1+1+1+1$ of 4. For example, the conjugacy class in S_4 with cycle type $2+2$ is $\{(12)(34), (13)(24), (14)(23)\}$.

Besides formula $\ast$ there are a few other simple permutation identities which do a lot for our understanding of S_n:

LEMMA 2 Let a & b be distinct elements of X and let A and B be (possibly empty) sequences of distinct elements of X, disjoint from each other and from a & b. Then

$$(1)\quad (aAbB)(ab) = (aB)(bA),$$

so

$$(2)\quad (aB)(bA)(ab) = (aAbB).$$

Proof (1) Since cycles are maps, the second factor acts first. For example, if $B=\phi$, then $(\cdots)$ takes a to b to a, i.e. fixes a, giving the cycle (a). But if $B \neq \phi$, say $B=(b_1, \ldots b_\ell)$, then $(\cdots)$ takes a to b to b_1; takes b_1 to b_2, ..., takes b_ℓ to a, giving the cycle (aB). Writing $(aAbB) = (bBaA)$, as we may, the same argument shows that the effect of $(\cdots)$ on b and A is the same as the cycle (bA).
(2) follows from (1), since $(ab)(ab) = 1$.

COR. For a & b distinct and disjoint from B,

$$(3)\quad (abB)(ab) = (aB).$$

Also, for $\ell \geq 2$,

$$(4)\quad (1\,2 \ldots \ell) = (1\ell)\ldots(12).$$

Proof (3) Take $A=\phi$ in (1) and use $(b)=1$.
(4) Use (3) with $B=(3\ldots\ell)$ (so $C=\phi$ for $\ell=2$),

$$(1\,2\ldots\ell)(12) = (1\,3\ldots\ell).$$

Similarly

$$(1\,3\ldots\ell)(13) = (1\,4\ldots\ell), \text{ etc.}$$

until

$$(1\,2\ldots\ell)\underbrace{(12)(13)\cdots(1\,\ell\text{-}1)} = (1\ell),$$

from which (4) follows by multiplying by the inverse of $\underbrace{\cdots}$.

THM C. S_n is generated by the set of all <u>transpositions</u> (ab) with $1 \le a < b \le n$.

Proof. For $n=1$, $S_n = 1 = \langle \phi \rangle$, which is fortunate because there are no transpositions in S_1. For $n \geqslant 2$, it suffices to observe that each l-cycle with $l \geqslant 2$ is a product of transpositions, by (4).

LEMMA 3. Let $\pi \in S_n$. Denote by $\nu(\pi)$ the number of cycles (including 1-cycles) in the disjoint cycle factorization of π. Then for each transposition $\tau \in S_n$,

$$(5) \qquad \nu(\pi\tau) = \nu(\pi) \pm 1.$$

Proof. Let $\tau = (ab)$. Then a & b either occur in the same cycle $(aAbB)$ of π or in different cycles (aB) & (bA). We may write these last in either case. Then by (1) and (2) in Lemma 2, $\pi\tau$ ends with $(aB)(bA)$ or $(aAbB)$, the other cycles in π appearing unchanged in $\pi\tau$. Thus $\nu(\pi\tau) = \nu(\pi)+1$ or $\nu(\pi)-1$.

DEF The <u>sign</u> $\varepsilon(\pi)$ of an element $\pi \in S_n$ is defined by

$$(6) \qquad \varepsilon(\pi) = (-1)^{n-\nu(\pi)}.$$

THM D We have $\varepsilon(1) = 1$ and for each $\pi \in S_n$ and each transposition τ,

$$(7) \qquad \varepsilon(\pi\tau) = -\varepsilon(\pi),$$

so

$$(8) \qquad \varepsilon(\pi) = (-1)^t$$

if π can be written as a product of t transpositions. This implies:

(9) The parity of t is determined by π, though t itself is not.

(10) $\varepsilon : S_n \to \{\pm 1\}$ is a surjective homomorphism, for $n \geqslant 2$.

Proof. $\varepsilon(1) = 1$ since $\nu(1) = n$. Also, (7) follows from (5) and (6). If $\pi = \tau_1 \cdots \tau_t$ (a product of t transpositions), then by (7) repeatedly

$$\varepsilon(\pi) = \varepsilon(\tau_1 \cdots \tau_{t-1}\tau_t) = -\varepsilon(\tau_1 \cdots \tau_{t-1}) = \cdots = (-1)^t,$$

giving (8). The implication (8) $\Longrightarrow$ (9) is because π determines $\varepsilon(\pi)$. And (8) $\Longrightarrow$ (10):

$$\varepsilon(\pi\pi') = \varepsilon(\tau_1 \cdots \tau_t \tau'_1 \cdots \tau'_{t'}) = (-1)^{t+t'} = (-1)^t(-1)^{t'} = \varepsilon(\pi)\varepsilon(\pi').$$

DEF The *alternating group* A_n is the kernel of ε. Thus $A_n = 1$ for $n = 1$ and for $n \geq 2$, A_n is the normal subgroup of index 2 in S_n consisting of all *even* permutations, i.e. those $\pi \in S_n$ which can (only!) be written as a product of an even number of transpositions.

THM E A_n is generated by the set of all 3-cycles.

Proof. For $n = 1$ & $n = 2$, $A_n = 1 = \langle \phi \rangle$, o.k. since there are no 3-cycles. For $n \geq 3$, it suffices by THM C to show that each product of two transpositions is either 1, or a 3-cycle, or a product of two three-cycles. This follows from

$$(12)(12) = 1, \quad (12)(23) = (123), \quad (12)(34) = (123)(234)$$

(easily checked), which cover the cases of total, partial, or no overlap in the two transpositions.

THM F. (1) For $n \geq 5$, each 3-cycle $\gamma \in S_n$ can be written $\gamma = \alpha\beta\alpha^{-1}\beta^{-1}$ for some 3-cycles $\alpha, \beta \in S_n$.
(2) For $n \geq 5$, A_n has no normal subgroup $K \neq A_n$ with A_n/K abelian.

Proof (1) It suffices to deal with the case $\gamma = (123)$. Put $\alpha = (124)$, $\beta = (135)$. Then $\alpha\beta\alpha^{-1} = (235)$, e.g. by lemma 1, so $\alpha\beta\alpha^{-1}\beta^{-1} = (235)(153) = (123) = \gamma$.
(2). By (1) and THM E each element of A_n is a product of *commutators* $\alpha\beta\alpha^{-1}\beta^{-1}$ with $\alpha, \beta \in A_n$. If $K \triangleleft A_n$ with A_n/K abelian, then $\alpha K \beta K = \beta K \alpha K$ for all $\alpha, \beta \in A_n$, so $\alpha\beta\alpha^{-1}\beta^{-1}K = \alpha K \beta K (\beta K \alpha K)^{-1} = K$, showing $\alpha\beta\alpha^{-1}\beta^{-1} \in K$, so $A_n \subset K$ so $K = A_n$.

THM G. S_5 is generated by $\{\sigma, \tau\}$, for any 5-cycle σ and any transposition τ.

Proof. We may suppose that $\tau = (12)$ and, after replacing σ by some power of σ, we may suppose that $\sigma = (12345)$. It suffices to show that $\langle \sigma, \tau \rangle$ contains all transpositions, i.e. (ij) for $1 \leq i < j \leq 5$. By lemma 1,

$$\tau^{\sigma} = (23), \quad (23)^{\sigma} = (34), \quad (34)^{\sigma} = (45)$$

and

$$(12)^{(23)} = (13), \quad (13)^{(34)} = (14), \quad (14)^{45} = (15),$$

so $\langle \sigma, \tau \rangle$ contains $(1j)$ for $1 < j \leq 5$. Finally, for $1 < i < j \leq 5$, Lemma 1 gives

$$(ij) = (1j)^{(1i)}.$$

Therefore $\langle \sigma, \tau \rangle$ contains all transpositions and is therefore all of S_5, by THM C.