- **semigroup:** A set with an associative binary operation.
- **group:** A set with an associative binary operation, which has a neutral (identity) element, and every element has an inverse.
- **subgroup:** For a group G and $H \subseteq G$

$$H \leq G \iff \begin{cases} 1 \in H \\ x, y \in H \Rightarrow xy \in H \\ x \in H \Rightarrow x^{-1} \in H \end{cases} \iff \begin{cases} 1 \in H \\ x, y \in H \Rightarrow xy^{-1} \in H \end{cases}$$

- **generated subgroup:** For a subset $S \subseteq G$,

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H = \{\, s_1^{\varepsilon_i} s_2^{\varepsilon_2} \cdots s_m^{\varepsilon_m} \mid s_i \in S,\ \varepsilon_i = \pm 1 \,\}$$

- **normal subgroup:** $N \triangleleft G \iff N \leq G$ and $g^{-1}ng \in N\ \forall n \in N$ ($\iff Ng = gN$ for any $g \in G$)
  ($\iff$ there is a homomorphism φ from G such that $N = \operatorname{Ker} \varphi$)
- **order of a group:** number of elements, $|G|$
- **order of an element:** $o(g)$ is the smallest positive integer k such that $g^k = 1$. $o(g) = \infty$ if no such k exists. (Equivalently, $o(g) = |\langle g \rangle|$)
- **cyclic groups:** $\langle g \rangle$ (notation: C_n or C_∞)
- **dihedral groups:** D_n is the group of symmetries (=isometries) of a regular n-gon (n rotations, n reflections)
- **symmetric groups S_Ω and S_n:** S_Ω is the group of bijections $\Omega \to \Omega$ (that is, permutations of Ω), where the operation is the composition from left to right. The permutations act an the right: $\omega \mapsto \omega g$.
  S_n if $|\Omega| = n$, usually, $\Omega = \{\, 1, 2, \ldots, n \,\}$
- **alternating group A_n:** the group of even permutations in S_n.
  $A_n \triangleleft S_n$, $|S_n : A_n| = 2$.
- **$GL_n(K)$:** multiplicative group of invertible $n \times n$ matrices over the field K
- **$SL_n(K)$:** multiplicative group of $n \times n$ matrices over K with determinant 1.
  $SL_n(K) \triangleleft GL_n(K)$
- **cycles:** $g = (a_1 a_2 \ldots a_k) \in S_\Omega$, where $a_1, \ldots, a_k$ are distinct elements of Ω. g maps $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$ and $b \mapsto b$ for every other $b \in \Omega$.
- **disjoint cycle decomposition (dcd):** product of cylces with no common element (it is unique up to the order of the cycles and rotations of the cycles themselves)
- **operations with permutations in dcd:**
  - product: apply the permutations from left to right
  - kth power: take the kth power of each cycle in the dcd (using k steps instead of one)
  - inverse: substitute each cycle in the dcd with the reverse cycle
  - order: the least common multiple of the cycle lengths in dcd
- **even and odd permutations:** A permutation g is even
  - $\iff$ the corresponding permutation matrix $M(g)$ has determinant 1
  - $\iff$ g can be written as a product of an even number of transpositions
  - $\iff$ a (not necessarily disjoint) cyclic decomposition of g has an even number of cycles of even length).

  A permutation is odd if it is not even.
- **transpositions:** 2-cycles
- **set product:** For $X, Y \subseteq G$: $XY := \{\, xy \mid x \in X,\ y \in Y \,\} \subseteq G$.
- **cosets:** For $H \leq G$ and $g \in G$, $Hg := H\{\, g \,\}$ is a right coset, $gH := \{\, g \,\} H$ is a left coset containing g.

- **index of a subgroup:** For $H \leq G$, the index $|G : H|$ is the number of right cosets (the same as the number of left cosets) of H in G. If G is finite then $|G : H| = |G|/|H|$.
- **transversal:** For $H \leq G$ a subset $R \subseteq G$ is a right transversal for H if every right coset contains exactly one element of R (equivalently, G is the disjoint union of the cosets Hr ($r \in R$). The left transversal is defined similarly.
- **factor group:** For $N \triangleleft G$, the factor group $G/N = \{ Ng \mid g \in G \}$ with the set product as operation.
  For this, $NaNb = Nab$, $N1 = N$ is the identily element, and $(Na)^{-1} = Na^{-1}$.
- **complement of a normal subgroup:** For $N \triangleleft G$, $\leq G$ is a complement of N if $NH = G$ and $N \cap H = 1$ (equivalently, $H \leq G$ is a transversal for N)
- **homomorphism and isomorphism:** $\varphi : G \to H$ is a group homomorphism if $\varphi(gg') = \varphi(g)\varphi(g')$ for every $g, g' \in G$. A bijective homomorphism is an isomorphism.
- **kernel and image:** For a homomorphism $\varphi : G \to H$,
  $\operatorname{Ker}\varphi = \{ g \in G \mid \varphi(g) = 1 \} \triangleleft G$
  $\operatorname{Im}\varphi = \{ h \in H \mid \exists g \in G : \ \varphi(g) = h \} \leq H$
- **conjugation:** $g^h = h^{-1}gh$. For every h conjugation by h is an automorphism of G (that is, isomorphism from G to G)
- **conjugacy classes:** The conjugacy class of g in G is $g^G := \{ g^h \mid h \in G \}$.
  G is the disjoint union of its conjugacy classes.
- **conjugation of permutations:** If $g : \alpha \mapsto \beta$ then $h^{-1}gh = g^h$ maps αh to βh. From the dcd of g we get the dcd of g^h by applying h on the elements of the cycles of g.
- **cycle structures and partitions in S_n:** Cycle structure: describes how many cycles and what lengths appear in the dcd of the permutation. To this belongs a partition of n into a sum of positive integers, 1's belonging to fixed-points.

Theorems and propositions

- **Disjoint cycle decomposition (dcd):** $|\Omega| < \infty \Rightarrow g \in S_\Omega$ can be written as a product of disjoint cycles and this decomposition is unique up to cyclic permutations of the elements in each cycle, and up to the order of the cycles.
- **Subgroups and orders of elements of a cyclic group:**
  P Every subgroup of a cyclic group is cyclic,
  and for every $0 < d \mid n$
  - a) there is exactly one subgroup of order d in C_n;
  - b) the number of elements of order d in C_n is $\varphi(d)$.
- **Order of a permutation:** If $g = c_1 \cdots c_k$ is a dcd, and c_i is of length n_i then $o(g) = \operatorname{lcm}(n_1, \ldots, n_k)$.

P **Lagrange Theorem:** If $|G| < \infty$ and $H \leq G$, then $|H| \mid |G|$.
(More generally: $|G| = |H| \cdot |G : H|$ for any G and $H \leq G$.)
- **Order of group and element:** If $|G| < \infty$ and $g \in G$ then $o(g) \mid |G|$.
- **Order of a homomorphic image of an element:** If $\varphi : G \to H$ is a homomorphism, $g \in G$ and $o(g) < \infty$ then $o(\varphi(g)) \mid \gcd(o(g), |H|)$.

P **Homomorphism Theorem:** If $\varphi : G \to H$ is a hom., then $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.
- **Normal subgroups and kernels:** $N \triangleleft G \Leftrightarrow \exists$ hom. $\varphi : G \to H$ such that $N = \operatorname{Ker}\varphi$.
- **Complement of a normal subgroup** If a normal subgroup $N \triangleleft G$ has a complement $H \leq G$, i.e. $N \cap H = 1$ and $NH = G$, then $G/N \cong H$.
- **Action of conjugation:** The conjugation by $g \in G$ is an isomorphism from G to G, so it preserves product, inverses and orders of elements.
- **Conjugacy as an equivalence relation:** G is the disjoint union of its conjugacy classes.

P **Conjugacy classes of S_n:** $g, h \in S_n$ are conjugate
$\Leftrightarrow$ their cycle structures are the same

$\Leftrightarrow$ they belong to the same partition of n.

- 1^{st} **Isomorphism Theorem:** If $N \triangleleft G$ and $H \leq G$ then $NH/N \cong H/N \cap H$.
- 2^{nd} **Isomorphism Theorem:** If $M \leq N \leq G$ and $M, N \triangleleft G$ then $G/N \cong (G/M)/(N/M)$.
- **Order of an element in G/N:** for $\bar{g} := Ng \in G/N$ $o(\bar{g})$ is the smallest pos. int. k such that $g^k \in N$. If no such k exists then $o(\bar{g}) = \infty$.
- **Normal subgroups of S_4:** The only normal subgroups of S_4 are 1 ,V, A_4 and S_4.

Other important facts from the problem sheets

2/6, 3/3, 5, 6.a), 4/6, 5/4