# $D_M$ - 07 MA-217 Discrete Mathematics / Jan-Apr 2007

**Lectures :** Tuesday/Thursday 15:45–17:15 ; Lecture Hall-1, Department of Mathematics

## 8. Group Actions — Symmetric Group, Pólya's enumeration Theorems

**8.1.** Let $I$ be a finite set with $\mathrm{card}(I) = n \in \mathbb{N}^+$ and let $n_1, \ldots, n_r$ be fixed natural numbers with $n_1 + \cdots + n_r = n$. Let $(I_1, \ldots, I_r)$ be a fixed partition of $I$ in $r$ pairwise disjoint subsets $I_k$, $k = 1, \ldots, r$ with $\mathrm{card}(I_k) = n_k$ for each $k = 1, \ldots, r$.

**a).** Show that $H := \{f \in \mathfrak{S}(I) \mid f(I_k) = I_k \text{ for } k = 1, \ldots, r\}$ is a subgroup of $\mathfrak{S}(I)$ of order $n_1! \cdots n_r!$.

**b).** Let $\mathfrak{Par}(I; n_1, \ldots, n_r)$ be the set of all partitions $(J_1, \ldots, J_r)$ of $I$ into pairwise disjoint subsets $J_1, \ldots, J_r$ such that $\mathrm{card}(J_k) = n_k$, $k = 1, \ldots, r$. Show that the map $\varphi : \mathfrak{S}(I) \to \mathfrak{Par}(I; n_1, \ldots, n_r)$ defined by $f \mapsto (f(I_1), \ldots, f(I_r))$ is surjective and the fibres of $\varphi$ are left cosets of $H$ in $\mathfrak{S}(I)$. Deduce that $\mathrm{card}(\mathfrak{Par}(I; n_1, \ldots, n_r)) = \dfrac{n!}{n_1! \cdots n_r!}$.

**c).** Find $\mathrm{card}\,(\{\sigma \in \mathfrak{S}_n \mid \mathrm{Fix}(\sigma) = \emptyset\})$. (**Hint :** Use Sylvester's-Sieve Formula (see Exercise 1.1). — **Remark :** This is a famous problem which was first solved by NICOLAS BERNOULLI (1687-1759) and later, independently, by LEONARD EULER (1707-1783).)

**d).** For $\sigma \in \mathfrak{S}_n$ with $\mathrm{ord}(\sigma) = p^m$ with $p$ prime, show that $\mathrm{card}(\mathrm{Fix}(\sigma)) \equiv n \pmod p$. In particular, (i) if $p \mid n$, then $\mathrm{Fix}(\sigma) \neq \emptyset$. (ii) if $p \mid n$, then $p \mid \mathrm{card}(\mathrm{Fix}(\sigma))$.

**8.2.** (Conjugacy classes in $\mathfrak{S}(I)$) Let $I$ be a finite set of cardinality $n \in \mathbb{N}^+$.

**a).** The elements $\sigma$ and $\rho$ in $\mathfrak{S}(I)$ are conjugates if and only if they have the same cycle-type (see T8.1-5)), i.e. $\nu(\sigma) = \nu(\rho)$.

**b).** Show that $\sigma$ is an even permutation if and only if $\nu_2 + \nu_4 + \cdots + \nu_{2[n/2]} \equiv 0 \pmod 2$, where $\nu(\sigma) = (\nu_1, \ldots, \nu_n)$.

**c).** Show that the number of conjugacy classes in the symmetric group $\mathfrak{S}_n$ is equal to the number $P(n) := \mathrm{card}\{(\nu_1, \nu_2, \ldots, \nu_n) \in \mathbb{N}^n \mid 1\nu_1 + 2\nu_2 + \cdots n\nu_n = n\}$ of partitions of $n$. (**Remark :** The number of conjugacy classes in a group $G$ is called the class number of $G$ and is denoted by $\mathrm{cl}(G)$ (see also T8.2-3)). Therefore $\mathrm{cl}(\mathfrak{S}(I)) = P(n)$. For small values of $n$, the number of partitions $P(n)$ of $n$ are give in the table below :

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $P(n)$ | 1 | 1 | 2 | 3 | 5 | 7 | 11 | 15 | 22 | 30 | 42 | 56 | 77 | 101 | 135 | 176 |

**8.3.** Let $I$ be a finite set of cardinality $n \in \mathbb{N}^+$. Let $\sigma \in \mathfrak{S}(I)$, $\nu = \nu(\sigma) = (\nu_1, \nu_2, \ldots, \nu_n) \in \mathbb{N}^n$ be the cycle-type (see T8.1-5)) of $\sigma$ and let $\mathrm{Z}_{\mathfrak{S}(I)}(\sigma) := \{\rho \in \mathfrak{S}(I) \mid \sigma\rho = \rho\sigma\}$ denote the *centraliser* of $\sigma$ in $\mathfrak{S}(I)$.

**a).** Show that $\mathrm{Z}_{\mathfrak{S}(I)}(\sigma)$ is a subgroup of $\mathfrak{S}(I)$ of index (the number of distinct left-cosets of the subgroup $\mathrm{Z}_{\mathfrak{S}(I)}(\sigma)$ in $\mathfrak{S}(I)$)) $[\mathfrak{S}(I) : \mathrm{Z}_{\mathfrak{S}(I)}(\sigma)] = \mathrm{card}(\{\rho \mid \nu(\rho) = (\nu_1, \nu_2, \ldots, \nu_n)\}) = \dfrac{n!}{\nu_1!\nu_2! \cdots \nu_n! \cdot 1^{\nu_1} 2^{\nu_2} \cdots n^{\nu_n}}$ and is of order $\mathrm{card}(\mathrm{Z}_{\mathfrak{S}(I)}(\sigma)) = \nu_1!\nu_2! \cdots \nu_n! \cdot 1^{\nu_1} 2^{\nu_2} \cdots n^{\nu_n}$. Deduce that the number cycles of length $k$ in the symmetric group $\mathfrak{S}(I)$ is $\dfrac{n!}{k \cdot (n-k)!}$.

**b).** If $\rho \in \mathrm{Z}_{\mathfrak{S}(I)}(\sigma)$, then $\rho(\mathrm{Fix}(\sigma)) \subseteq \mathrm{Fix}(\sigma)$.

**c).** If $\sigma = \langle 1, 2, \cdots, k\rangle$ is a cycle of length $k$, then $\rho \in \mathrm{Z}_{\mathfrak{S}(I)}(\sigma)$ if and only if $\rho = \langle 1, 2, \cdots, k\rangle^r \tau$ with $0 \leq r \leq k$ and $\tau \in \mathfrak{S}(I)$ with $\mathrm{Supp}(\tau) \cap \{1, 2, \ldots, k\} = \emptyset$. Deduce that $\mathrm{Z}_{\mathfrak{S}(I)}(\langle 1, 2, \cdots, n\rangle) = \mathrm{H}(\langle 1, 2, \cdots, n\rangle)$ is the subgroup of $\mathfrak{S}(I)$ generated by $\langle 1, 2, \cdots, n\rangle$.

**d).** Let $p$ be a prime number. Then show that $\text{card}(\{\sigma \in \mathfrak{S}_p \mid \sigma^p = \text{id}\}) = (p-1)! + 1$. of the subgroup

**8.4.** Let $n \in \mathbb{N}^+$.

**a).** Find an injective group homomorphism $f : \mathfrak{S}_n \to \mathfrak{A}_{n+2}$. (**Hint:** For $\sigma \in \mathfrak{S}_n$, let $\widetilde{\sigma} := \begin{cases} \sigma, & \text{if } \sigma \text{ is even,} \\ \sigma \cdot (n+1\, n+2), & \text{if } \sigma \text{ is odd.} \end{cases}$ Then $\widetilde{\sigma} \in \mathfrak{A}_{n+2}$ and the map $\sigma \mapsto \widetilde{\sigma}$ is an injective group homomorphism.)

**b).** Find an injective group homomorphism $g : \mathfrak{S}_n \to \mathfrak{A}_{2n}$ and deduce that every finite group $G$ is isomorphic to a subgroup of the alternating group $\mathfrak{A}_m$ for some $m \in \mathbb{N}^+$. (**Hint:** For $\sigma \in \mathfrak{S}_n$, let $\sigma^{\#} := \begin{cases} \sigma(k), & \text{if } 1 \le k \le n, \\ \sigma(k-n)+n, & \text{if } n+1 \le k \le 2n. \end{cases}$ Then $\sigma^{\#} \in \mathfrak{A}_{2n}$ and the map $\sigma \mapsto \sigma^{\#}$ is an injective group homomorphism.)

**c).** For $\sigma \in \mathfrak{S}_n$, let $\mathfrak{P}_\sigma$ denote the $n \times n$-matrix obtained from the $n \times n$ identity matrix $\mathfrak{E}_n$ by permuting its columns according as the permutation $\sigma$; the matrix $\mathfrak{P}_\sigma$ is called the permutation matrix corresponding to the permutation $\sigma$. Further, the matrix $\mathfrak{P}_\sigma$ is invertible, i.e., $\mathfrak{P}_\sigma \in \text{GL}_n(K)$, in fact $(\mathfrak{P}_\sigma)^{-1} = \mathfrak{P}_{\sigma^{-1}}$. Then the map $\psi : \mathfrak{S}_n \to \text{GL}_n(K)$, $\sigma \mapsto \mathfrak{P}_\sigma$ is an injective homomorphism of groups and that $\sigma \in \mathfrak{A}_n$ (resp. $\sigma \notin \mathfrak{A}_n$) if and only if $\text{Det}(\psi(\sigma)) = 1$ (resp. $\text{Det}(\psi(\sigma)) = -1$).

**8.5.** Let $G$ be a group and let $X$ be a $G$-set. Show that

**a).** (Burnside's Formula) $\text{card}(G) \cdot \text{card}(X/G) = \sum_{g \in G} \text{card}(\text{Fix}_g(X))$. (**Hint:** Let $Y := \{(g,x) \in G \times X \mid gx = x\}$. Look at the fibres of the mappings $Y \to G$, $(g,x) \mapsto g$ and $Y \to X$, $(g,x) \mapsto x$.)

**b).** Suppose that $G$ is finite. For $g \in G$, let $n(g) = \text{card}(\text{Fix}_g(X))$. Show that

(1) If $G$ acts transitively on $X$ then $\text{card}(G) = \sum_{g \in G} n(g)$. Deduce that, if $\text{card}(X) \ge 2$ and $G$ acts transitively on $X$ then there exists $g \in G$ such that $\text{Fix}_g(G) = \emptyset$. (**Hint:** Use the Burnside's formula.)
(2) If $G$ acts 2-transitively on $X$ then $2 \cdot \text{card}(G) = \sum_{g \in G} n(g)^2$. (**Hint:** Use T8.2-6)-c) and the part (1) above.)

**8.6.** Let $G$ be a finite group of order $n \in \mathbb{N}^+$ which operates on itself by the left-translation and let $\lambda : G \to \mathfrak{S}(G)$ be the corresponding Cayley's homomorphism.

**a).** For every $g \in G$, show that the permutation $\lambda_g$ has exactly $n/\text{ord}(g)$ orbits each of cardinality $\text{ord}(g)$. In particular, $\text{Sign}(\lambda_g) = (-1)^{n-(n/\text{ord}(g))} = (-1)^{[G:\text{H}(g)]+|G|}$, where $\text{H}(g)$ is the cyclic subgroup of $G$ generated by $g$

**b).** If $G = \mathfrak{S}_n$ with $n \ge 4$, then show that the image $\lambda(\mathfrak{S}_n)$ is contained in the kernel of the group homomorphism $\text{Sign} : \mathfrak{S}(\mathfrak{S}_n) \to \{1, -1\})$. (**Hint:** Note that since $n \ge 4$, $4 \big| n! = \text{Ord}(G)$. Use part a) to compute $\text{Sign}(\tau)$ for a transpositions $\tau \in \mathfrak{S}_n$.)

**c).** Show that the image $\lambda(G)$ is not contained in the kernel of the group homomorphism $\text{Sign} : \mathfrak{S}(G) \to \{1, -1\})$, i.e., $\lambda(G) \not\subseteq \mathfrak{A}(G)(= \mathfrak{A}_n)$ if and only if $n$ is even and that $G$ has an element of order $2^\alpha$, where $\alpha := v_2(n)$ (this second condition is equivalent to: a 2-Sylow subgroup of $G$ is cyclic and is non-trivial. For Sylow subgroups see T8.2-20).) Moreover, in this case $G$ has a normal subgroup of index 2. (**Hint:** The kernel of the group homomorphism $\text{Sign} \circ \lambda : G \longrightarrow \lambda(G) \longrightarrow \{1, -1\}$ is a normal subgroup of $G$ of index 2.)

**d).** If $\text{ord}(G) = 2m$ with $m$ odd then show that $G$ has a normal subgroup of index 2. (**Hint:** Since $2 \big| 2m$, there exists $g \in G$ with $\text{ord}(g) = 2$ by Cauchy's theorem (see T8.2-2)-e)-(1)). Compute the $\text{Sign}(\lambda_g)$ by using part a) and use c). — **Remark:** From this and the famous theorem of Feit-Thompson: *Every finite non-abelian simple group has even order.* (See [Feit, W. and Thompson, J.:

Solvability of groups of odd order, *Pacific Journal of Mathematics*, pp-775-1029, (1963).]) one easliy proves that: *If $G$ is non-abelian and simple* (i.e., $G$ has no proper normal subgroup), *then* 4 *divides* $\mathrm{ord}(G)$. The proof of the theorem of Feit-Thompson is not easy.)

**8.7.** Let $T$ be a set of transpositions in the group $\mathfrak{S}_n$, $n \geq 1$. We associate the graph (see T8.4) $\Gamma_T$ to $T$ as follows: the vertices of $\Gamma_T$ are the numbers $1, \ldots, n$ and two vertices $i$ and $j$ with $i \neq j$ are joined by a edge if and only if the transposition $\langle i, j\rangle = \langle j, i\rangle$ belong to $T$. Let $\Gamma_1, \ldots, \Gamma_r$ be the connected components of $\Gamma_T$.

**a).** The transpositions in $T$ generate the group $\mathfrak{S}_n$ if and only if $\Gamma_T$ is connected, i.e. if any two vertices of $\Gamma_T$ can be joined by the sequence of edges in $\Gamma_T$. The subgroup of $\mathfrak{S}_n$ generated by $T$ is the product $\mathfrak{S}(\Gamma_1) \times \cdots \times \mathfrak{S}(\Gamma_r) \subseteq \mathfrak{S}_n$.

**b).** If $T$ is a generating system for the group $\mathfrak{S}_n$, then $T$ has at least $n-1$ elements. (**Hint:** Let $\tau_1, \ldots, \tau_m$ be the elements of $T$ (may be with repeatations) with $\tau_1 \cdots \tau_m = \mathrm{id}$. Then $m$ is even and $m \geq 2\sum_{\rho=1}^{r}(|\Gamma_\rho| - 1)$. )

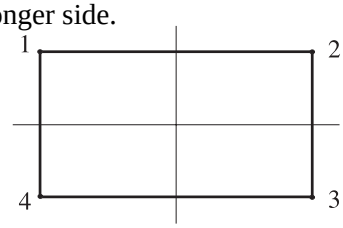
**c).** Every generating system of $\mathfrak{S}_n$ consisting of transpositions contain a (minimal) generating system of $\mathfrak{S}_n$ with $n-1$ elements. (**Hint:** Prove this by descending induction $k$; induction starts at $k = n-1$: the number of trees in which the number 1 belongs to exactly $k$ edges, is $(n-1)^{n-k-1}\binom{n-2}{k-1}$ and add. — **Remarks:** The graphs corresponding to such a minimal generating systems are called t r e e s. Every connected graph has a generating system which is a tree. –There are exactly $n^{n-2}$ generating systems consisting $n-1$ transpositions.)

**d).** The transpositions $\langle 1, 2\rangle, \langle 2, 3\rangle, \ldots, \langle n-1, n\rangle$ (resp. $\langle 1, 2\rangle, \langle 1, 3\rangle, \ldots, \langle 1, n\rangle$) form a minimal generating system of $\mathfrak{S}_n$. (**Hint:** If $a$, $b$, $c$ are three distinct elements, then $\langle a\,b\rangle\langle a\,c\rangle\langle a\,b\rangle = \langle b\,c\rangle$.)

**8.8. a).** Let $\vartheta : \mathrm{D}_n \to \mathfrak{S}_n$ be the action homomorphism of the canonical action of the dihedral group $\mathrm{D}_n$ on the set $\{1, 2, \ldots, \}$. Show that the cycle-polynomial of $\mathrm{D}_n$ with respect to $\vartheta$ is $\Psi(\mathrm{D}_n) = \frac{1}{2n}\sum_{d|n}\varphi(d)Z_d^{n/d} + \begin{cases} \frac{1}{4}(Z_1^2 + Z_2)Z_2^{(n-2)/2}, & \text{if } n \equiv 0 \pmod 2, \\ \frac{1}{2}Z_1 Z_2^{(n-1)/2}, & \text{if } n \equiv 1 \pmod 2, \end{cases}$ where $\varphi$ is the Euler's totient function.

**b).** Let $K$ be a finite field of cardinality $q$ and characteristic $p > 0$ and let $\mathrm{UT}_p(K) = \{\mathfrak{U} = \big(u_{ij}\big)_{1\leq i,j\leq p} \in \mathbb{M}_p(K) \mid u_{ij} = 0 \text{ for all } j < i \text{ and } u_{ii} = 1 \text{ for all } i = 1, \ldots, p\}$ be the set of all unipotent upper triangular $p \times p$ matrices over $K$. Find the cycle- polynomial of $\mathrm{UT}_p(K)$. (**Hint:** Note that $n := \mathrm{card}(\mathrm{UT}_p(K)) = q^{\binom{p}{2}}$ and every element $\mathfrak{U} \in \mathrm{UT}_p(K)$, $\mathfrak{U} \neq \mathfrak{E}_p$ has order $p$, since $\mathfrak{U}^p = \mathfrak{E}_p$ (use Cayley-Hamilton theorem and $\mathrm{Char}K = p$), where $\mathfrak{E}_p$ denote the $p \times p$ identity matrix over $K$. Therefore (see T8.3-2)-b)) $\Psi(\mathrm{UT}_p(K)) = \frac{1}{n}\left(Z_1^n + (n-1)Z_p^{n/p}\right)$.)

**c).** Find the cycle polynomial of the group $G$ of symmetries of the rectangle (which is not a square) (in the Euclidean plane $\mathbb{R}^2$). (**Hint:** Label the corners of the rectangle by 1, 2, 3, 4 (clockwise), where $\overline{12}$ is the longer side.

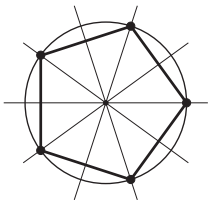


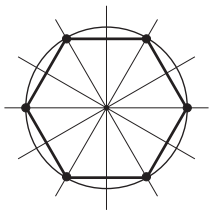

The symmetry group $G$ of the rectangle consists of the following 4 permutations: id, $\langle 1, 3\rangle\langle 2, 4\rangle$ (a rotation through angle $\pi$, $\langle 1, 2\rangle\langle 3, 4\rangle$ (a reflection in perpendicular axis), $\langle 1, 4\rangle\langle 2, 3\rangle$ (a reflection in parallel axis). Therefore $\Psi(G) = \frac{1}{4}(Z_1^4 + 3Z_2^2)$.)

**d).** Find the cycle polynomial of the group W of face permutations induced by the rotational symmetries of the cube. (**Hint:** Show that the group W is isomorphic to the symmetric group $\mathfrak{S}_4$ and use the table in T8.1-5)-c)-2) to conclude that $\Psi(\mathrm{W}) = \frac{1}{24}(Z_1^6 + 3Z_1^2Z_2^2 + 6Z_1^2Z_4 + 6Z_2^3 + 8Z_3^2)$.)

**8.9.** Let $\mathrm{R}_n$ be a regular $n$-gon in the real plane $\mathbb{R}^2$, $n \geq 3$ and let $Y$ be a finite set (of colors).

**a).** On the set $Y^{\mathrm{R}_n}$ of all colourings of $\mathrm{R}_n$, consider the equivalence relation $\sim$ : Two colourings $f, g \in Y^{\mathrm{R}_n}$ are said to be equivalent under $\sim$, i.e., $f \sim g$ if there exists a rotation $\rho : \mathrm{R}_n \to \mathrm{R}_n$ of the regular $n$-gon $\mathrm{R}_n$ such that $g(v) = f(\sigma^{-1}(v))$ for every $v \in \mathrm{V}(\mathrm{R}_n) =$ (the vertex set of $\mathrm{R}_n$). The elements of the quotient set $Y^{\mathrm{R}_n}/\sim$ are called patterns of colourings of $\mathrm{R}_n$ with respect to the rotations.

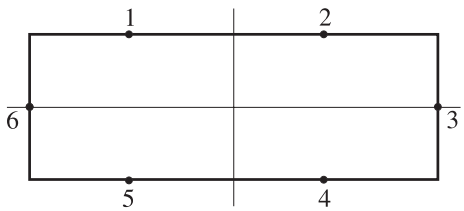

$n = 5$


$n = 6$

Show that the total number of patterns with at most $m$ colours is $\frac{1}{n}\sum_{d|n}\varphi(d)m^{n/d}$ and the number of patterns $[f] \in Y^{\mathrm{R}_n}$ such that exactly $\alpha_i$ vertices in $\mathrm{R}_n$ in the colouring $f$ have been assigned the colour $i$ is $\displaystyle\frac{1}{n}\sum_{d\,|\,\gcd(\alpha_1,\ldots,\alpha_m)} \varphi(d)\frac{(n/d)!}{(\alpha_1/d)!\cdots(\alpha_m/d)!}$. (If $\gcd(\alpha_1,\ldots,\alpha_m) = 1$, then this number is $\displaystyle\frac{(n-1)!}{\alpha_1!\cdots\alpha_m!}$; for a regular 6-gon, there are $\frac{1}{6}(2^6+2^3+2\cdot2^2+2\cdot2^1) = 14$ patterns with at most 2 colours (and 12 patterns with exactly 2 colours). — **Hint :** For each colour $i \in Y$, consider the weight $\gamma(i) := T_i$, where $T_i$, $i \in Y$, are indeterminates over $\mathbb{Q}$; therefore we have the weight function $\gamma : Y^{\mathrm{R}_n} \to \mathbb{Q}[T_1,\ldots,T_m]$ defined by $f \mapsto \gamma(f) := T_1^{\alpha_1}\cdots T_m^{\alpha_m}$, where $\alpha_i$ is the number of vertices in the colouring $f$ has assigned the colour $i$, i.e., $\alpha_i := \mathrm{card}(\{v \in V(\mathrm{R}_n) \mid f(v) = i\})$ for each $i = 1,\ldots,m$. Note that if $f \sim g$ for $f, g \in Y^{\mathrm{R}_n}$, then $\gamma(f) = \gamma(g)$ and hence we have a well-defined weight function $\overline{\gamma} : Y^{\mathrm{R}_n}/\sim \longrightarrow \mathbb{Q}[T_1,\ldots,T_m]$, $[f] \mapsto \gamma(f)$. Now, by T8.3-3)-b) the coefficient of $T_1^{\alpha_1}\cdots T_m^{\alpha_m}$ in the polynomial $\Psi(G)(\pi_1,\ldots,\pi_n) = \displaystyle\frac{1}{n}\sum_{d|n}\varphi(d)(T_1^d+\cdots+T_m^d)^{n/d}$ is the number of patterns $[f] \in Y^{\mathrm{R}_n}$ such that exactly $\alpha_i$ vertices in $\mathrm{R}_n$ in the colouring $f$ has assigned the colour $i$, where $\Psi(G)\left(= \Psi(\mathrm{Z}_n) = \frac{1}{n}\sum_{d|n}\varphi(d)Z_d^{n/d}\right)$ (see T8.3-1)-c)) is the cycle-polynomial of the group of rotations $G$ of the regular $n$-gon $\mathrm{R}_n$ with respect to its natural action on the vertex set $\mathrm{V}(\mathrm{R}_n) = \{v_1,\ldots,v_n\}$ and $\pi_j := \sum_{i=1}^m T_1^j + \cdots + T_m^j$, for $j = 1,\ldots,n$ (see also T8.3). Further by using the polynomial theorem (since $\alpha_1+\cdots+\alpha_m = n$ and $\alpha = \gcd(\alpha_1,\ldots\alpha_m)$) show that this number is $\displaystyle\frac{1}{n}\sum_{d\,|\,\gcd(\alpha_1,\ldots,\alpha_m)} \varphi(d)\frac{(n/d)!}{(\alpha_1/d)!\cdots(\alpha_m/d)!}$.)

**b).** Find the number of different patterns of necklaces consisting of $n$ pearls of $m$ distinct colours of which exactly $\alpha_i$ pearls are of the colour $i$ for every $i = 1\ldots,m$, $\alpha_1+\cdots+\alpha_m = n$, when (1) only rotational symmetries (of a regular $n$-gon $\mathrm{R}_n$ with $n$ vertices) are considered; and (2) both rotational and reflectional symmetries (of a regular $n$-gon $\mathrm{R}_n$ with $n$ vertices) are considered. (**Hint :** (1) is similar to a) and for (2) use Exercise 8.8-a). For $n = 6$ and $m = 2$, there are $7 + (3\cdot 8)/4 = 13$ patterns with at most 2 colours and 11 patterns with exactly 2 colours. — **Remark :** For necklaces which are not closed, one can give a much simpler solution to this problem!)

**c).** Find the number of inequivalent way of seating 4 men and 2 women at a reactangular dining table if seats are situated as in the figure below :



**d).** Show that the number patterns of colourings of the sides of the cube (in $\mathbb{R}^3$) using at most $m$ colours if the colour $i$ is used exactly $\alpha_i$ times is the coefficient $T_1^{\alpha_1}\cdots T_m^{\alpha_m}$ in the polynomial $\Psi(\mathrm{W})(\pi_1,\ldots,\pi_n)$, where $\Psi(\mathrm{W}) = \frac{1}{24}(Z_1^6+3Z_1^2Z_2^2+6Z_1^2Z_4+6Z_2^3+8Z_3^2)$ (see Exercise 8.8-d)) and $\pi_j = \sum_{i=1}^m T_i^j$, $j = 1,2,3,4$. In particular, the total number of patterns is $\frac{m^2}{24}(m^4+3m^2+12m+8)$; for $m=2$ this number is 10 (resp. is 8 if both the colours are used). (1) In how many ways (with reswpct to the rotational symmetries of the cube) can the facses of the cube be painted red, blue or gree, if each colour must be used at least once? (Since $m=3$ and hence the total number of ways is $\Psi(\mathrm{W})(3,3,3,3) = 57$ and with at most two colours $\Psi(\mathrm{W})(2,2,2,2) = 10$ and hence the required the number is $57-3\cdot 10 = 27$.) (2) Among 57 total patterns in (1), how many involve 0 red, (resp. 1 red, 2 red, ..., 6 red) faces? (Give weights $T$, 1, 1 to the colours red, blue, green, respectively, then the cofeeicint of $T^\alpha$, $\alpha = 0,1,2,3,4,5,6$ is the required answer.) (**Remark:** Let the colours are denoted by natural numbers $i \in \mathbb{N}$ and give weight $T^i$ ($T$ indeterminate over $\mathbb{Q}$) to the colour $i \in \mathbb{N}$. Then $\pi_j = \sum_{i\in\mathbb{N}}(T^i)^j = \sum_{i\in\mathbb{N}} T^{ij} = \frac{1}{1-T^j}$ and the coefficient of $T^\alpha$ in the power series $\Psi(\mathrm{W})\left(\frac{1}{1-T},\frac{1}{1-T^2},\frac{1}{1-T^3},\frac{1}{1-T^4}\right)$ is the number of distinct numbering (colouring) with natural numbers such that the total sum is $\alpha$, $\alpha \in \mathbb{N}$.)

**8.10.** Let $\Gamma = (V,E)$ be a graph with the set of $n$- vertices $V = \{1,\ldots,n\}$ and the set of edges $E \subseteq \mathfrak{P}_2(\{1,\ldots,n\})$. Two graphs $\Gamma = (V,E)$ and $\Gamma' = (V,E')$ with the same set of vertices are said to be isomorphic or equivalent if there exists a permutation $\sigma \in \mathfrak{S}_n$ such that the map (induced by $\sigma$) $E \to E'$, $(i,j) \mapsto (\sigma(i),\sigma(j)$ is bijective; in this case we write $\Gamma = (V,E) \cong_\sigma \Gamma = (V,E')$. Then the relation "isomorphism of graphs" (on the set of all graphs with the same vertex set $\{1,\ldots,n\}$) is an equivalence relation; its equivalence classes are called the isomorphism classes of graphs with the vertex set $\{1,\ldots,n\}$.

**a).** On the set $\mathfrak{P}_2(\{1,\ldots,n\})$ the permutation group $\mathfrak{S}_n$ acts in a natural way (see T8.2-9)-c) and hence acts naturally on the set $\{0,1\}^{\mathfrak{P}_2(\{1,\ldots,n\})}$ of indicators functions. Show that there is a bijection from the isomorphism classes of of graphs with the vertex set $\{1,\ldots,n\}$ onto the quotient set $\{0,1\}^{\mathfrak{P}_2(\{1,\ldots,n\})}/\mathfrak{S}_n$. (**Hint:** A subset (edge-set) of $\mathfrak{P}_2(\{1,\ldots,n\})$ is identified with its indicator function in $\{0,1\}^{\mathfrak{P}_2(\{1,\ldots,n\})}$.)

**b).** Suppose that we are given two colours 0 with weight 1 and 1 with weight $T$ (an indeterminate over $\mathbb{Q}$). Show that the number of isomorphism classes of the graphs with vertex set $\{1,\ldots,n\}$ and $\alpha$ edges, $\alpha \in \mathbb{N}$ is the coefficient of $T^\alpha$ in the polynomial $\Psi_n(1+T,1+T^2,\ldots,1+T^n)$, where $\Psi_n$ is the cycle-polynomial of the symmetric group $\mathfrak{S}_n$ with respect to the natural action of $\mathfrak{S}_n$ on the set $\mathfrak{P}_2(\{1,\ldots,n\})$. Further, show that the total number of isomorphism classes of the graphs with vertex set $\{1,\ldots,n\}$ is $\Psi_n(2,\ldots,2)$. For $n=4$, $\mathrm{card}(\mathfrak{P}_2(\{1,\ldots,n\})) = \binom{4}{2} = 6$, and (since the natural action of $\mathfrak{S}_4$ on $\mathfrak{P}_2(\{1,\ldots,n\})$ is transitive) the cycle-polynomial of with respect to this action is $\Psi_4 = \frac{1}{24}\left(Z_1^6+9Z_1^2Z_2^2+6Z_2Z_4+8Z_3^2\right)$ (see table (2) in T8.2- 5)). In particular, there are $\Psi_4(2,2,2,2) = 11$ distinct isomorphism classes of graphs with 4 vertices. Give a representative in each of this isomorphism class.

**c).** Compute the number of isomorphism classes of the graphs with $n$ vertices for $n = 5,6,7,8,9,10$. (**Remarks:** For $n=10$, there are 12005168 isomorphism classes of graphs with 10 vertices. — For more examples of this type see the book: [Kerber, A.: Algebraic Combonatorics Via Finite Group Actions, Manheim, 1991].)

---

Below one can see Class-Notes and (simple) test-exercises.

## Class-Notes/Test-Exercises

**T8.1.** (Symmetric group) For a (finite) set $I$, let $\mathfrak{S}(I) := \{\sigma \in I^I \mid \sigma \text{ is bijective}\}$. Then the composition $\circ$ of maps is a binary operation on $\mathfrak{S}(I)$ and with respect to this binary operation $\mathfrak{S}(I)$ is a group; the neutral (identity) element in this group is the identity map $\mathrm{id}_I$ and for $\sigma \in \mathfrak{S}(I)$ the inverse map of $\sigma$ (which exists since $\sigma$ is bijective) is the inverse of the element $\sigma$ in the group $\mathfrak{S}(I)$; for $\sigma, \rho \in \mathfrak{S}(I)$, we write $\sigma\rho$ for the composition $\sigma \circ \rho$. This group $(\mathfrak{S}(I), \circ)$ is called the symmetric group or permutation group on the set $I$; its elements are called permutations on $I$. For $n \in \mathbb{N}^+$, we put $\mathfrak{S}_n := \mathfrak{S}(\{1, 2, \ldots, n\})$.

**1).** An arbitrary finite group $G$ is a subgroup of a permutation group. More presicely,

**a).** Cayley's Theorem. *Let $G$ be a group. For $g \in G$, let $\lambda_g : G \to G$, $x \mapsto gx$ denote the left-multiplication on $G$ by $g$. Then the map $\lambda : G \to \mathfrak{S}(G)$, $g \mapsto \lambda_g$ is an injective group homomorphism.* This group homomorphism $\lambda$ is called the Cayley's representation [1]) of $G$. (**Proof:** First note that $\lambda_g$ is bijective, i.e. $\lambda_g \in \mathfrak{S}(I)$, in fact, the left-multiplication $\lambda_{g^{-1}}$ is the inverse map of $\lambda_g$, since $\lambda_g\lambda_{g^{-1}} = \lambda_{gg^{-1}} = \lambda_e = \mathrm{id}_G = \lambda_{g^{-1}}\lambda_g$. Further, for $g, g' \in G$ and $x \in G$, we have $\lambda_{gg'}(x) = (gg')x = g(g'x) = \lambda_g(\lambda_{g'}(x)) = (\lambda_g\lambda_{g'})(x)$ and hence $\lambda(gg') = \lambda_{gg'} = \lambda_g\lambda_{g'} = \lambda(g)\lambda(g')$ which proves that $\lambda$ is a group homomorphism. Finally, if $\lambda(g) = \lambda(g')$ for some $g, g' \in G$, then $g = ge = \lambda(g)(e) = \lambda(g')(e) = g'e = g'$ and hence $\lambda$ is injective.)

**b).** If $I = \{i\}$, then $\mathfrak{S}(I) = \{\mathrm{id}_I\}$; if $I = \{i, j\}$ with $i \neq j$, then $\mathfrak{S}(I) = \{\mathrm{id}_I, \sigma\}$ where $\sigma(i) = j$; if $\mathrm{card}(I) \geq 3$, then $\mathfrak{S}(I)$ is not abelian, in fact, the center $\mathrm{Z}(\mathfrak{S}(I)) = \{\rho \in \mathfrak{S}(I) \mid \sigma\rho = \rho\sigma\} = \{\mathrm{id}_I\}$. (**Proof:** For $\sigma \in \mathfrak{S}(I)$ with $\sigma \neq \mathrm{id}_I$. We shall show that $\sigma \notin \mathrm{Z}(\mathfrak{S}(I))$. Choose $i \in I$ with $j := \sigma(i) \neq i$ (since $\sigma \neq \mathrm{id}_I$). Further, since $\mathrm{card}(I) \geq 3$, there exists $k \in I \setminus \{i, j\}$. Let $\tau \in \mathfrak{S}(I)$ be defined by $\tau(j) = k$, $\tau(k) = j$ and $\tau(a) = a$ for all $a \in I \setminus \{j, k\}$. Then $\sigma\tau(i) = \sigma(i) = j$ and $\tau\sigma(i) = \tau(j) = k \neq j$ and hence $\sigma\tau \neq \tau\sigma$. This proves that $\sigma \notin \mathrm{Z}(\mathfrak{S}(I))$.)

**c).** Let $I$ and $I'$ be two sets with $\mathrm{card}(I) = \mathrm{card}(I')$, i.e. there is a bijective map $f : I \to I'$. Then the map $\Phi_f : \mathfrak{S}(I) \to \mathfrak{S}(I')$ defined by $\sigma \mapsto f\sigma f^{-1}$ is an isomorphism of groups. In particular, if $I$ is a set with $\mathrm{card}(I) = n$, then the groups $\mathfrak{S}(I)$ and $\mathfrak{S}_n$ are isomorphic.

**d).** The order of the symmetric group $\mathfrak{S}(I)$ is $\mathrm{card}(I)!$.

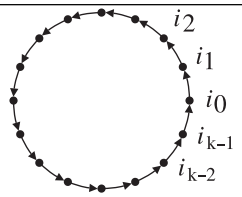
**2).** (Support, fixed points and orbits of a permutation) For a permutation $\sigma \in \mathfrak{S}(I)$, the subset $\mathrm{Supp}(\sigma) := \{i \in I \mid \sigma(i) \neq i\}$ is called the support of $\sigma$ and the subset $\mathrm{Fix}(\sigma) := \{i \in I \mid \sigma(i) = i\}$ is called the fixed set of $\sigma$.

**a).** $\sigma(\mathrm{Supp}(\sigma)) \subseteq \mathrm{Supp}(\sigma)$ for every $\sigma \in \mathfrak{S}_n$. Further, two permutations $\sigma, \rho \in \mathfrak{S}(I)$ are called disjoint if $\mathrm{Supp}(\sigma)\,\mathrm{Supp}(\rho) = \emptyset$; in this case they commute, i.e., $\sigma\rho = \rho\sigma$ and $\mathrm{Supp}(\sigma\rho) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$. If $\sigma_1, \ldots, \sigma_m \in \mathfrak{S}(I)$ are permutations with pairwise disjoint supports, i.e., $\mathrm{Supp}(\sigma_i) \cap \mathrm{Supp}(\sigma_j) = \emptyset$ for every $i \neq j$. Then $\sigma_1, \ldots, \sigma_m$ are pairwise commutative, i.e., $\sigma_i\sigma_j = \sigma_j\sigma_i$ for all $1 \leq i, j \leq m$.

**b).** (Orbits of a permutation) For a fixed $i \in I$, the set $\mathrm{O}_\sigma(i) := \{\sigma^m(i) \mid m \in \mathbb{Z}\}$ is called the orbit of $i$ under $\sigma$. (1) For $i, j \in I$, show that either $\mathrm{O}_\sigma(i) = \mathrm{O}_\sigma(j)$ or $\mathrm{O}_\sigma(i) \cap \mathrm{O}_\sigma(j) = \emptyset$. Therefore the orbits of $\sigma$ form a partition of $I$. (2) Let $s$ be the smallest positive natural number such that $i_0 := i, i_1 := \sigma(i_0), i_2 := \sigma(i_1) = \sigma^2(i_0), \ldots, i_{s-1} := \sigma(i_{s-2}) = \sigma^2(i_{s-3}) = \cdots = \sigma^{s-1}(i_0)$ are distinct, then $\sigma^s(i_0) = i_0 = i$ and $\mathrm{O}_\sigma(i) = \{i_0, i_1, \ldots, i_{s-1}\} = \{\rho(i) \mid \rho \in \mathrm{H}(\sigma)\}$, where $\mathrm{H}(\sigma) := \{\sigma^r \mid r \in \mathbb{Z}\}$ is the (cyclic) subgroup of $\mathfrak{S}(I)$ generated by $\sigma$. (**Proof:** From $\sigma^s(i) = \sigma^k(i)$ with $0 \leq k < s$, it follows that $\sigma^{s-k}(i) = \sigma^{-k}(\sigma^s(i)) = \sigma^{-k}(\sigma^k(i)) = i = i_0$ and hence $k = 0$ by the choice of $s$, since $0 < s - k \leq s$. For the last equality, let $\sigma^r \in \mathrm{H}(\sigma)$ and $r = qs + k$ with $0 \leq k < s$, $q \in \mathbb{Z}$. Then $\sigma^r(i) = \sigma^k((\sigma^s)(i)) = \sigma^k(i) = i_k$.)

**c).** A permutation $\sigma \in \mathfrak{S}(I)$ is called a cycle if has exactly one orbit with cardinality $\geq 2$. In this case its support $\mathrm{Supp}(\sigma) = \mathrm{O}(i) = \{i = i_0, i_1, \ldots, i_{s-1}\}$ for some $i \in I$; the cardinality $s = \mathrm{card}(\mathrm{O}(i)) = \mathrm{card}(\mathrm{Supp}(\sigma))$ is called the length of $\sigma$, denoted by $\ell(\sigma)$. Further, if $\sigma \neq \mathrm{id}_I$, then $s > 0$ and $\sigma$ is denoted by $\langle i_0, i_1, \cdots, i_{s-1}\rangle$.

[1]) This is named after English mathematician ARTHUR CAYLEY (1821-1895).




Note that $\langle i_0, i_1, \cdots, i_{s-1}\rangle = \langle i_k, i_{k+1}, \cdots, i_{s-1}, i_0, \cdots, i_{k-1}\rangle$ for all $k = 1, \ldots, s-1$. Further, the order of the cycle $\langle i_0, i_1, \cdots, i_{s-1}\rangle$ in the group $\mathfrak{S}(I)$ is its length $s$ and its inverse $\sigma^{-1} = \langle i_{s-1}, i_{s-2}, \cdots, i_1, i_0\rangle$ is also cycle of length $s$.

The cycles of length 2 are called transpositions. A transposition $\langle i, j\rangle \in \mathfrak{S}(I)$, $i \neq j$, which interchange elements $i$ and $j$ and fix the remaining elements of $I$. A cycle $\langle i_0, i_1, \ldots, i_{k-1}\rangle$ of length $k$ is the product of $k-1$ transpositions: $\langle i_0, i_1, \ldots, i_{k-1}\rangle = \langle i_0, i_1\rangle \langle i_1, i_2\rangle \cdots \langle i_{k-2}, i_{k-1}\rangle$.

**3).** (Canonical decomposition of a permutation) *Let $I$ be a finite set. Then every permutation $\sigma \in \mathfrak{S}(I)$ has a representation $\sigma = \sigma_1 \cdots \sigma_r$ with cycles $\sigma_1, \ldots, \sigma_r \in \mathfrak{S}(I)$ of lengths $\geq 2$ and the supports are pairwise disjoint. Moreover, this representation is unique upto the order of the factors.* (**Remark:** For the proof of the uniqueness we need that the supports of the cycles $\sigma_1, \ldots, \sigma_r$ are the orbits of $\sigma$ contain mor than one element. For example, the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 17 & 3 & 11 & 5 & 4 & 2 & 19 & 12 & 9 & 15 & 7 & 1 & 10 & 18 & 20 & 14 & 8 & 16 & 6 & 13 \end{pmatrix} \in \mathfrak{S}_{20}$ has the canonical cycle decomposition $\langle 1, 17, 8, 12\rangle \langle 2, 3, 11, 7, 19, 6\rangle \langle 4, 5\rangle \langle 10, 15, 20, 13\rangle \langle 14, 18, 16\rangle$. The support $\mathrm{Supp}(\sigma) = \{1, \ldots, 20\} \setminus \{9\}$.)

**a).** *The order of $\sigma$ is:* $\mathrm{Ord}\,\sigma = \mathrm{lcm}\,(\mathrm{Ord}\,\sigma_1, \ldots, \mathrm{Ord}\,\sigma_r) = \mathrm{lcm}\,\big(\ell(\sigma_1), \ldots, \ell(\sigma_r)\big)$. The above permutation $\sigma \in \mathfrak{S}_{20}$ has the order $\mathrm{Ord}\,\sigma = \mathrm{lcm}\,(4, 6, 2, 4, 3) = 12$. (**Proof:** From the cycle decomposition $\sigma = \sigma_1 \cdots \sigma_r$, it follows that $\sigma^m = \sigma_1^m \cdots \sigma_r^m$, $m \in \mathbb{Z}$, since $\sigma_i \sigma_j = \sigma_j \sigma_i$ for all $1 \leq i, j \leq r$, $i \neq j$. Therefore only to note that the order of a cycle is equal to its length.)

**b).** The canonical cycle decomposition of the inverse $\sigma^{-1}$ of $\sigma$ is $\sigma^{-1} = \sigma_r^{-1} \cdots \sigma_1^{-1} = \sigma_1^{-1} \cdots \sigma_r^{-1}$, where $\sigma = \sigma_1 \cdots \sigma_r$ is the canonical decomposition of $\sigma$ and for a cycle $\langle i_0, \ldots, i_{k-1}\rangle$ of length $k$, the inverse $\langle i_0, \ldots, i_{k-1}\rangle^{-1} = \langle i_{k-1}, i_{k-2}, \ldots, i_0\rangle = \langle i_0, i_{k-1}, \ldots, i_1\rangle$ is again a cycle of length $k$. The canonical decomposition of the inverse $\sigma^{-1}$ of the above permutation $\sigma \in \mathfrak{S}_{20}$, is $\sigma^{-1} = \langle 1, 12, 8, 17\rangle \langle 2, 6, 19, 7, 11, 3\rangle \langle 4, 5\rangle \langle 10, 13, 20, 15\rangle \langle 14, 16, 18\rangle$.

**c).** *Let $I$ be a finite set. Then every permutation $\sigma$ on $I$ has a representation as a product of transpositions.* (**Proof:** Immediate from the fact that every permutation $\sigma \in \mathfrak{S}(I)$ is a product of cycles. — **Remark:** One can also prove this directly: Let $\sigma \in \mathfrak{S}(I)$, $\sigma \neq \mathrm{id}$ and let $\sigma(i_0) = j_0 \neq i_0$. Then $\sigma' := \langle i_0, j_0\rangle \sigma$ is a permutation with $i_0$ as a fixed point. Then by induction on $\mathrm{card}(I)$ the permutation $\sigma' | (I \setminus \{i_0\}) \in \mathfrak{S}(I \setminus \{i_0\})$ has a representation $\sigma' = \langle i_1, j_1\rangle \cdots \langle i_s, j_s\rangle$ as a product of transpositions and hence $\sigma = \langle i_0, j_0\rangle \sigma' = \langle i_0, j_0\rangle \langle i_1, j_1\rangle \cdots \langle i_s, j_s\rangle$. The representation of a permutation as a product of transpositions (in contrast with the canonical cycle-decomposition) is naturally not unique. For example, each such a representation can be extended by using $\mathrm{id}_I = \tau\tau$ with any transposition $\tau$. However, we shalll see below that the parity of the number of transpositions in any representation of $\sigma$ into transpositions is uniquely determined. We have noted above by using the canonical cycle decomposition one can get such a representation into exactly $n - s$ transpositions, where $n$ : $\mathrm{card}(I)$ and $s$ is the number of orbits of $\sigma$ (singleton orbits are also counted!).)

**d).** A bijective map $f : I \to I'$ induce (see 1)-c)) an isomorphism of groups $\Phi_f : \mathfrak{S}(I) \to \mathfrak{S}(I')$ mit $\sigma \mapsto f\sigma f^{-1}$. The $k$-cycle $\langle a_1, \ldots, a_k\rangle$ is mapped onto the $k$-cycle $\langle f(a_1), \ldots, f(a_k)\rangle$. Therefore (if $I$ is finite), the cycle decomposition of $f\sigma f^{-1}$ is obtained by replacing the cycles in the cycle decomposition of $\sigma$ by its $f$- images. *In particular, for $\sigma, \rho \in \mathfrak{S}(I)$, the cycle decomposition of the permutation $\rho\sigma\rho^{-1}$ is obtained replacing the elements in the cycles in the cycle decomposition of the permutation $\sigma$ by their $\rho$-images.*

**4).** (Sign of a permutation) Let $\sigma$ be a permutation on the set $I$ with cardinality $n \in \mathbb{N}^+$ and let $s$ be the number of orbits of $\sigma$. Then the signature of $\sigma$ is defined by the formula: $\mathrm{Sign}\,\sigma := (-1)^{n-s}$. The permutation $\sigma$ is called even if $\mathrm{Sign}\,\sigma = 1$, otherwise it is called odd. If $I_1, \ldots, I_s$ are orbits of $\sigma$, then $n - s = \sum_{k=1}^{s} |I_k| - s = \sum_{k=1}^{s} \big(|I_k| - 1\big)$ and hence $\mathrm{Sign}\,\sigma = \prod_{k=1}^{s} (-1)^{|I_k|-1}$. Therefore note that: $\mathrm{Sign}\,\sigma = (-1)^g$, *where $g$ is the number of orbits of $\sigma$ with even-cardinality.*

**a).** The identity permutation is even. A transposition is odd; more generally, a cycle of length $k$ has the signature $(-1)^{k-1}$. The permutation $\sigma \in \mathfrak{S}_{20}$ in 3) above is even, since it has exactly 4 orbits of even-cardinality.

**b).** The following theorem is the most basic: *Let $I$ be a finite set. suppose that the permutation $\sigma \in \mathfrak{S}(I)$ is a product $\sigma = \tau_1 \cdots \tau_k$ of $k$ transpositions $\tau_1, \ldots, \tau_k$. Then* $\operatorname{Sign}\sigma = (-1)^k$. *In particular, the number of factors int a representation of a even (resp. odd) permutation as a product of transpositions is always even (resp. odd).* (**Proof:** (by induction on $k$). It is enough to prove that $\sigma$ and $\tau\sigma$ have different signatures for an arbitrary transposition $\tau$. For this it is enough to show that the number of orbits of $\sigma$ and $\tau\sigma$ differ by 1. Let $\tau = \langle i, j\rangle$. Either both $i$ and $j$ are contained in the same orbit or different orbit of $\sigma$, we shall consider these two cases separately. Case 1: Suppose that both $i$ and $j$ lie in the same orbit of $\sigma$. Then the canonical cycle decomposition of $\sigma$ is of the form $\sigma = \langle i_0, \ldots, i_r, \ldots, i_{s-1}\rangle \cdots$ with $i_0 = i$ and $i_r = j$ and hence $\tau\sigma = \langle i_0, \ldots, i_{r-1}\rangle\langle i_r, \ldots, i_{s-1}\rangle \cdots$, and the number of orbits of $\tau\sigma$ is 1 more than that of $\sigma$. Case 2: Suppose that $i$ and $j$ lie in the different orbits of $\sigma$. Then the canonical cycle decomposition of $\sigma$ is of the form $\sigma = \langle i_0, \ldots, i_{r-1}\rangle\langle j_0, \ldots, j_{s-1}\rangle \cdots$ with $i_0 = i$ and $j_0 = j$ and hence $\tau\sigma = \langle i_0, \ldots, i_{r-1}, j_0, \ldots, j_{s-1}\rangle \cdots$. and the number of orbits of $\tau\sigma$ is 1 less than that of $\sigma$. )

**c).** *Let $I$ be a finite set. Then the map* $\operatorname{Sign}: \mathfrak{S}(I) \longrightarrow \{1, -1\}$ *is a group homomorphism,* i.e., *for $\sigma, \tau \in \mathfrak{S}(I)$, we have* $\operatorname{Sign}\sigma\tau = (\operatorname{Sign}\sigma)(\operatorname{Sign}\tau)$. (**Proof:** Write $\sigma = \sigma_1 \cdots \sigma_s$ and $\tau = \tau_1 \cdots \tau_t$ as product of transpositions $\sigma_1, \ldots, \sigma_s$ resp. $\tau_1, \ldots, \tau_t$ and from the representation $\sigma\tau = \sigma_1 \cdots \sigma_s\tau_1 \cdots \tau_t$ and b) above we get $\operatorname{Sign}\sigma\tau = (-1)^{s+t} = (-1)^s(-1)^t = (\operatorname{Sign}\sigma)(\operatorname{Sign}\tau)$.)

**d).** (The alternating group) Let $I$ be a finite set. Then the subgroup of $\mathfrak{S}(I)$ consisting of even permutations of $I$ is called the alternating group on $I$ and is denoted by $\mathfrak{A}(I)$. — The alternating group on the set $\{1, \ldots, n\}$ is simply denoted by $\mathfrak{A}_n$. Note that $\mathfrak{A}(I)$ is the kernel of the group homomorphism Sign and hence is normal in $\mathfrak{S}(I)$. Further, if $n := \operatorname{card}(I) \geq 2$, then the index of $\mathfrak{A}(I)$ in $\mathfrak{S}(I)$ is 2. The two cosets of $\mathfrak{A}(I)$ in $\mathfrak{S}(I)$ is the set $\mathfrak{A}(I)$ of even permutations and the set $\mathfrak{S}(I) \setminus \mathfrak{A}(I) = \tau\mathfrak{A}(I) = \mathfrak{A}(I)\tau$ of all odd permutations, where $\tau \in \mathfrak{S}(I)$ is an arbitrary odd permutation (e.g., a transposition) and hence $\operatorname{Ord}\mathfrak{A}(I) = n!/2$ (and the number of odd permutations is $n!/2$). For $n \geq 4$, show that the alternating group $\mathfrak{A}_n$ is not abelian.

**e).** (Inversions of a permutation) In the case $I = \{1, \ldots, n\}$ the signature of a permutation $\sigma \in \mathfrak{S}(I) = \mathfrak{S}_n$ can also be computed by using the well-known inversions. For $\sigma \in \mathfrak{S}(I)$ a pair $(i, j) \in I \times I$ is called a inversion of $\sigma$ if $i < j$, but $\sigma(i) > \sigma(j)$. The number of inversions of $\sigma$ is denoted by $\mathrm{z}(\sigma)$. For example, (1) The transposition $\langle i, j\rangle \in \mathfrak{S}_n$, $i < j$, has the inversions $(i, i+1), \ldots, (i, j)$; $(i+1, j), \ldots, (j-1, j)$ and hence $\mathrm{z}(\langle i, j\rangle) = 2(j-i) - 1$. (2) In the permutation $\sigma := \binom{1\ 2\ \ldots\ n}{n\ n-1\ \ldots\ 1} \in \mathfrak{S}_n$ all the pairs $(i, j)$ with $1 \leq i < j \leq n$ inversions and hence $\mathrm{z}(\sigma) = \binom{n}{2}$. (3) The permutation $\sigma := \binom{1\,2\,3\,4\,5}{3\,1\,5\,2\,4} \in \mathfrak{S}_5$ has the inversions $(1, 2)$, $(1, 4)$, $(3, 4)$ and $(3, 5)$ and hence $\mathrm{z}(\sigma) = 4$.

**f).** *Let $\sigma \in \mathfrak{S}_n$ be a permutation. Then* $\operatorname{Sign}\sigma = (-1)^{\mathrm{z}(\sigma)}$. (**Proof:** Since by example (1) in e) above a transposition has an odd number of inversions, it is enough to prove that: For $\sigma, \tau \in \mathfrak{S}_n$, $(-1)^{\mathrm{z}(\sigma\tau)} = (-1)^{\mathrm{z}(\sigma)}(-1)^{\mathrm{z}(\tau)}$. For $\sigma \in \mathfrak{S}_n$, clearly $(-1)^{\mathrm{z}(\sigma)} = \prod_{1\leq i<j\leq n} \operatorname{Sign}\big(\sigma(j) - \sigma(i)\big)$. Therefore $(-1)^{\mathrm{z}(\sigma\tau)} = \prod_{1\leq i<j\leq n} \operatorname{Sign}\big(\sigma(\tau(j)) - \sigma(\tau(i))\big) = (-1)^{\mathrm{z}(\tau)} \prod_{1\leq r<s\leq n} \operatorname{Sign}\big(\sigma(s) - \sigma(r)\big) = (-1)^{\mathrm{z}(\tau)}(-1)^{\mathrm{z}(\sigma)}$. The second equality follows from the fact that exactly there are $\mathrm{z}(\tau)$ pairs $\big(\tau(i), \tau(j)\big)$, $1 \leq i < j \leq n$ such that their components are interchanged and for this we need to consider the set of all pairs $(r, s)$, $1 \leq r < s \leq n$.)

**g).** By f) the sign of the permutation $\sigma \in \mathfrak{S}_n$ in the Example e)-(2) is $\operatorname{Sign}\sigma = (-1)^{\binom{n}{2}}$. This also follows from the canonical cycle decomposition $\sigma = \langle 1, n\rangle\langle 2, n-1\rangle \ldots \langle [n/2], n+1-[n/2]\rangle$ is the product of $[n/2]$ transpositions. Therefore $(-1)^{\left[\frac{n}{2}\right]} = (-1)^{\binom{n}{2}} = \begin{cases} 1, & \text{if } n \equiv 0, 1 \bmod 4, \\ -1, & \text{if } n \equiv 2, 3 \bmod 4. \end{cases}$

**h).** Let $I$ be a set with more than two elements. *Then the center of the permutation group $\mathfrak{S}(I)$ is trivial.* If $\sigma \in \mathfrak{S}(I)$, $\sigma \neq \mathrm{id}$, $\sigma(a) \neq a$ and $\tau$ is a transposition $\langle \sigma(a), c\rangle$ with $c \notin \{a, \sigma(a)\}$, then $\tau\sigma\tau^{-1}$ maps the element $a$ onto $c$ and hence $\tau\sigma\tau^{-1} \neq \sigma$ and $\sigma$ does not commute with $\tau$.

**i).** For the following permutations compute the number of inversions and the sign.

(i). The permutation $i \mapsto n-i+1$ in $\mathfrak{S}_n$. (ii). $\begin{pmatrix} 1 & 2 & \dots & n & n+1 & \dots & 2n \\ 1 & 3 & \dots & 2n-1 & 2 & \dots & 2n \end{pmatrix} \in \mathfrak{S}_{2n}$.

(iii). $\begin{pmatrix} 1 & 2 & \dots & n & n+1 & \dots & 2n \\ 2 & 4 & \dots & 2n & 1 & \dots & 2n-1 \end{pmatrix} \in \mathfrak{S}_{2n}$.

(iv). $\begin{pmatrix} 1 & \dots & n-r+1 & n-r+2 & \dots & n \\ r & \dots & n & 1 & \dots & r-1 \end{pmatrix} \in \mathfrak{S}_n,\ 1 \le r \le n$. (**Ans:** $(-1)^{(r-1)(n+1)}$.)

(v). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 2n \\ 1 & 2n & 3 & 2(n-1) & 5 & 2(n-2) & \dots & 2 \end{pmatrix} \in \mathfrak{S}_{2n}$.

(vi). For a subset $J \subseteq \{1, \dots, n\}$ with $J = \{j_1, \dots, j_m\}$, $j_1 < \cdots < j_m$, let $\sigma_J$ be the permutation

$$\sigma_J = \begin{pmatrix} 1 & \dots & m & m+1 & \dots & n \\ j_1 & \dots & j_m & i_1 & \dots & i_{n-m} \end{pmatrix} \in \mathfrak{S}_n,$$

where the numbers $i_1 < \cdots < i_{n-m}$ are the elements of the complement of $J$ in $\{1, \dots, n\}$. (**Hint:** The number of variations of $\sigma_J$ is $\mathrm{z}(\sigma_J) = \left(\sum_{k=1}^{m} j_k\right) - \binom{m+1}{2}$ and hence $\mathrm{Sign}\,(\sigma_J) = (-1)^{\mathrm{z}(\sigma_J)}$. )

(vii). Let $\sigma$ resp. $\tau$ be permutations of the finite sets $I$ resp. $J$. Compute the sign of the permutation $\sigma \times \tau : (i,\ j) \mapsto (\sigma\, i,\ \tau\, j)$ of $I \times J$ (in terms of $\mathrm{Sign}\,\sigma$, $\mathrm{Sign}\,\tau$ and $m := |I|$, $n := |J|$).

**j).** (i). A subgroup of the permutation group $\mathfrak{S}_n$ which contain an odd permutation contains equal number of even and odd permutations. (ii). A permutation $\sigma \in \mathfrak{S}_n$ which is of odd order is an even permutation. (iii). The square $\sigma^2$ of a permutation $\sigma \in \mathfrak{S}_n$ is an even permutation. (iv). Let $\sigma = \langle i_0, \dots, i_{k-1} \rangle$ be a cycle of length $k \ge 2$. For which $m \in \mathbb{Z}$, $\sigma^m$ is a cycle of length $k$? (v). Let $\sigma \in \mathfrak{S}_n$ and $m \in \mathbb{Z}$. Every orbit of $\sigma$ of length $k$ decomposes into ggT $(k, m)$ orbits of the length $k/\gcd(k, m)$ of $\sigma^m$. (vi). Let $I$ be a finite set. The inverse $\sigma^{-1}$ of a permutation $\sigma \in \mathfrak{S}(I)$ has the same orbits and same sign as those of $\sigma$. (vii). Let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the canonical prime factorisation of $m \in \mathbb{N}^*$. Then the permutation group $\mathfrak{S}_n$ contain an element of order $m$ if and only if $n \ge p_1^{\alpha_1} + \cdots + p_r^{\alpha_r}$. For which $n \in \mathbb{N}$ there exists an element of order 3000 (resp. 3001) in the group $\mathfrak{S}_n$? (viii). If $\sigma \in \mathfrak{S}_n$, $n \in \mathbb{N}^+$ has $s$ orbits, then $\sigma$ can be represented as a product of $n-s$ transpositions and cannot be represented as a product of less than $n-s$ transpositions.

**k).** (i). For $n \ge 2$, $\mathrm{Sign} : \mathfrak{S}_n \to \{-1, 1\}$ is the only non-trivial group homomorphism. (**Hint:** $\langle a\, b \rangle$ and $\langle c\, d \rangle$ be two transpositions $\mathfrak{S}_n$. If $\sigma \in \mathfrak{S}_n$ be an arbitrary permutation with $a \mapsto c$, $b \mapsto d$, then $\sigma \langle a\, b \rangle \sigma^{-1} = \langle c\, d \rangle$ and so every homomorphism $\varphi : \mathfrak{S}_n \to \{1, -1\}$ have the same value on all transpositions. If this value is 1, then $\varphi = \mathrm{id}$; if it is $-1$, then $\varphi = \mathrm{Sign}$.) (ii). $\mathfrak{A}_n$ is the commutator $\mathfrak{S}_n$. (iii). Using the simplicity of the group $\mathfrak{A}_n$, $n \ge 5$, prove that the group $\mathfrak{A}_n$ is the only non-trivial normal subgroup in the group $\mathfrak{S}_n$ for $n \ge 5$. (iv). The groups $\mathfrak{A}_4$ and $\mathfrak{V}_4$ are the only non-trivial normal subgroups in $\mathfrak{S}_4$. (v). The group $\mathfrak{V}_4$ is the only non-trivial normal subgroup in $\mathfrak{A}_4$.

**l).** (i). The cycles $\langle 1, 2 \rangle$, $\langle 2, \dots, n \rangle$ generate the group $\mathfrak{S}_n$, $n \ge 2$. (**Hint:** Use Exercise 8.7-d)) (ii). The cycles $\langle 1, 2 \rangle$, $\langle 1, 2, \dots, n \rangle$ generate the group $\mathfrak{S}_n$, $n \ge 2$. (**Hint:** Use Exercise 8.7-d)) (iii). $\langle 1, n \rangle$, $\langle 1, \dots, n \rangle$ generate the group $\mathfrak{S}_n$, $n \ge 2$. (**Hint:** Use Exercise 8.7-d))

**5).** (Cycle-type of a permutation) Let $I$ be a finite set with $\mathrm{card}(I) = n$ and let $\sigma \in \mathfrak{S}(I)$. For $k = 1, \dots, n$, let $\nu_k$ is the number of cycles of length $k$ in the cycle decomposition of $\sigma$. Then the $n$-tuple $\nu(\sigma) := (\nu_1, \dots, \nu_n)$ is called the cycle-type of $\sigma$.

**a).** The cycle type of the cycle of length $k$ is $(n-k, 0, \dots, 1, 0, \dots, 0)$, where 1 is at the $k$-place. In particular, the cycle type of the $n$-cycle in $\mathfrak{S}_n$ is $\nu(\langle 1, 2, \cdots, n \rangle) = (0, 0, \dots, 0, 1)$.

**b).** For a permutation $\sigma \in \mathfrak{S}(I)$, show that $\nu(\sigma^{-1}) = \nu(\sigma)$.

**c).** The cycle structure and cycle types in the groups $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{A}_4$, $\mathfrak{S}_5$, $\mathfrak{A}_5$.

(1) The group $\mathfrak{S}_3$ :

| Cycle type | Cycle Structure | Number | Order | Parity |
|---|---|---|---|---|
| $3e_1 = (3, 0, 0)$ | id | 1 | 1 | even |
| $e_1 + e_2 = (1, 1, 0)$ | $\langle 1, 2 \rangle$ | $3 = \frac{3\times 2}{2}$ | 2 | odd |
| $e_3 = (0, 0, 1)$ | $\langle 1, 2, 3 \rangle$ | $2 = \frac{3\times 2\times 1}{3}$ | 3 | even |
| | | $6 = \mathrm{card}(\mathfrak{S}_3)$ | | |

(2) The group $\mathfrak{S}_4$ :

| Cycle type | Cycle Structure | Number | Order | Parity |
|---|---|---|---|---|
| $4e_1 = (4,0,0,0)$ | id | 1 | 1 | even |
| $2e_1 + e_2 = (2,1,0,0)$ | $\langle 1,2\rangle$ | $6 = \frac{4\times3}{2}$ | 2 | odd |
| $e_1 + e_3 = (1,0,1,0)$ | $\langle 1,2,3\rangle$ | $8 = \frac{4\times3\times2}{3}$ | 3 | even |
| $e_4 = (0,0,0,1)$ | $\langle 1,2,3,4\rangle$ | $6 = \frac{4\times3\times2\times1}{4}$ | 4 | odd |
| $2e_2 = (0,2,0,0)$ | $\langle 1,2\rangle\langle 3,4\rangle$ | $3 = \frac{1}{2}\left(\frac{4\times3}{2} \times \frac{2\times1}{2}\right)$ | 2 | even |
| | | $24 = \text{card}(\mathfrak{S}_4)$ | | |

(3) The group $\mathfrak{A}_4$ :

| Cycle type | Cycle Structure | Number | Order | Parity |
|---|---|---|---|---|
| $4e_1 = (4,0,0,0)$ | id | 1 | 1 | even |
| $e_1 + e_3 = (0,1,1,0)$ | $\langle 1,2,3\rangle$ | $8 = \frac{4\times3\times2}{3}$ | 3 | even |
| $2e_2 = (0,2,0,0)$ | $\langle 1,2\rangle\langle 3,4\rangle$ | $3 = \frac{1}{2}\left(\frac{4\times3}{2} \times \frac{2\times1}{2}\right)$ | 2 | even |
| | | $12 = \text{card}(\mathfrak{A}_4)$ | | |

(4) The group $\mathfrak{S}_5$ :

| Cycle type | Cycle Structure | Number | Order | Parity |
|---|---|---|---|---|
| $5e_1 = (4,0,0,0,0)$ | id | 1 | 1 | even |
| $3e_1 + e_2 = (3,1,0,0,0)$ | $\langle 1,2\rangle$ | $10 = \frac{5\times4}{2}$ | 2 | odd |
| $2e_1 + e_3 = (2,0,1,0,0)$ | $\langle 1,2,3\rangle$ | $20 = \frac{5\times4\times3}{3}$ | 3 | even |
| $e_1 + e_4 = (1,0,0,1,0)$ | $\langle 1,2,3,4\rangle$ | $30 = \frac{5\times4\times3\times2}{4}$ | 4 | odd |
| $e_5 = (0,0,0,0,1)$ | $\langle 1,2,3,4,5\rangle$ | $24 = \frac{5\times4\times3\times2\times1}{5}$ | 5 | even |
| $e_1 + 2e_2 = (1,2,0,0,0)$ | $\langle 1,2\rangle\langle 3,4\rangle$ | $15 = \frac{1}{2}\left(\frac{5\times4}{2} \times \frac{3\times2}{2}\right)$ | 2 | even |
| $e_2 + e_3 = (0,1,1,0,0)$ | $\langle 1,2,3\rangle\langle 4,5\rangle$ | $20 = \frac{5\times4\times3\times2}{4}$ | 64 | odd |
| | | $120 = \text{card}(\mathfrak{S}_5)$ | | |

(5) The group $\mathfrak{A}_5$ :

| Cycle type | Cycle Structure | Number | Order | Parity |
|---|---|---|---|---|
| $5e_1 = (4,0,0,0,0)$ | id | 1 | 1 | even |
| $2e_1 + e_3 = (2,0,1,0,0)$ | $\langle 1,2,3\rangle$ | $20 = \frac{5\times4\times3}{3}$ | 3 | even |
| $e_5 = (0,0,0,0,1)$ | $\langle 1,2,3,4,5\rangle$ | $24 = \frac{5\times4\times3\times2\times1}{5}$ | 5 | even |
| $e_1 + 2e_2 = (1,2,0,0,0)$ | $\langle 1,2\rangle\langle 3,4\rangle$ | $15 = \frac{1}{2}\left(\frac{5\times4}{2} \times \frac{3\times2}{2}\right)$ | 2 | even |
| | | $60 = \text{card}(\mathfrak{A}_5)$ | | |

**T8.2.** (Operations (--actions) of Groups on sets --- action homomorphisms) Let $G$ be a (multiplicative) group with the identity element $e$. An operation or action of $G$ on a set $X$ is a map $G \times X \to X$ (called an operation map or action map) and denoted by $(g,x) \mapsto gx$ such that for all $g, h \in G$ and for all $x \in X$, we have: (1) $ex = x$ (2) $(gh)x = g(hx)$.

For a fixed $g \in G$, the map $\vartheta_g : X \to X$ defined by $x \mapsto gx$ is called the operation of $g$ on $X$ . Then $\vartheta_e = \text{id}_X$ and $\vartheta_{gh} = \vartheta_g\vartheta_h$ by the conditions (1) and (2) above, respectively. In particular, for every $g \in G$, the map $\vartheta_g$ is a permutation of $X$ and $(\vartheta_g)^{-1} = \vartheta_{g^{-1}}$. Therefore the map $\vartheta : G \to \mathfrak{S}(X)$ defined by $\vartheta(g) := \vartheta_g$ is a group homomorphism. This group homomorphism is called the action homomorphism of the action of $G$ on $X$. Conversely, if $\vartheta : G \to \mathfrak{S}(X)$ is a group homomorphism then the map $G \times X \to X$ defined by $(g,x) \mapsto \vartheta(g)(x)$ gives an operation on $X$.

A set $X$ with an action of a group $G$ is called a $G$ -set; the action homomorphism $\vartheta : G \to \mathfrak{S}(X)$ is called the action homomorphism of the $G$- set $X$.

**1).** (Orbits and isotropy subgroups --Stabilizers) Let $G$ be a group acting on a set $X$.

**a).** The operation of $G$ on $X$ defines an equivalence relation o $X$ : For $x, y \in X$, $x \sim_G y$ if and only if there exists $g \in G$ with $gx = y$.

**b).** The equivalence class of $x \in X$ under $\sim_G$ is denoted by $Gx := \{gx \mid g \in G\}$ and is called the orbit of $x$. The quotient set of all equivalence classes of the relation $\sim_G$ is denoted by $X/G$. We have the canonical surjective map $X \to X/G$, $x \mapsto Gx$ .

**c).** For $x \in X$, the subset $G_x := \{g \in G \mid gx = x\}$ is a subgroup of $G$. This subgroup is called the isotropy group or stabilizer of $x$.

**d).** For $x \in X$, the fibres of the cannonical surjective map $G \to Gx$ , $g \mapsto gx$ are the left-cosets of $G_x$ in $G$. In particular: (Orbit-Stabiliser theorem) $\text{card}(Gx) = [G : G_x]$, i.e., *the cardinality of the orbit $Gx$ of $x$ is the index $[G : G_x]$ of the isotropy subgroup of $x$ in $G$ and in particular, if $G$ is finite then* $\text{card}(Gx)$ *divides the order of the group $G$.*

**e).** For $g \in G$ and $x \in X$, $G_{gx} = gG_xg^{-1}$. i.e., *Isotropy subgroups of the elements in the same orbit are conjugate subgroups in $G$.*

**f).** An element $x \in X$ is called a fixed or invariant element with respect to the element $g \in G$ if $gx = x$. The set of fixed elements with respect to $g \in G$ is denoted by $\text{Fix}_g(X)$. If $E \subseteq G$ then we put $\text{Fix}_E(X) := \cap_{g\in E} \text{Fix}_g(X)$. The elements of $\text{Fix}_G(X)$ are called fixed elements of the operation of $G$ on $X$. An element $x \in X$ belongs to $\text{Fix}_G(X)$ if and only if $G_x = G$.

**g).** Let $V$ be a $n$-dimensional vector space over a field $K$, $n \in \mathbb{N}^+$ and let $G := \text{Aut}_K(V) = \text{GL}_K(V)$ be the automorphism group of $V$. In each of the following examples show that $G$ acts on the set $X$ with the action homomorphism $\vartheta : G \to \mathfrak{S}(X)$ . For $x \in X$ , describe the orbit $Gx$ of $x$ under $G$ geometrically (whenever possible) and find the isotropy subgroup $G_x$ at $x$.

(i). Let $X = V \setminus \{0\}$ and let $\vartheta : G \to \mathfrak{S}(V)$ be defined by $\vartheta(f)(v) := f(v)$ for $f \in G$ and $v \in V \setminus \{0\}$.

(ii). Let $X = \mathcal{B} := \{(v_1, \ldots, v_n) \in V^n \mid v_1, \ldots, v_n \text{ is a basis of } V\}$ and let $\vartheta : G \to \mathfrak{S}(\mathcal{B})$ be defined by $\vartheta(f)((v_1, \ldots, v_n)) := (f(v_1), \ldots, f(v_n))$ for $f \in G$ and $(v_1, \ldots, v_n) \in \mathcal{B}$.

(iii). Let $r \in \mathbb{N}$, $r \leq n$ and let $\text{G}_r(V)$ be the set of $r$-dimensional subspaces of $V$. Let $X = \text{G}_r(V)$ and let $\vartheta : G \to \mathfrak{S}(\text{G}_r(V))$ be defined by $\vartheta(g)(W) := g(W)$ for $g \in G$ and $W \in \text{G}_r(V)$.

(iv). Let $\mathcal{F}$ be the set of all flags $\{(0 = V_0 \subset V_1 \subset \cdots \subset V_n = V)\}$, where $V_i$ is a subspace of $V$, for $0 \leq i \leq n$. Let $X = \mathcal{F}$ and let $\vartheta : G \to \mathfrak{S}(\mathcal{F})$ be defined by $(V_0 \subset V_1 \subset \cdots \subset V_n) \mapsto (g(V_0) \subset g(V_1) \subset \cdots \subset g(V_n))$ for $g \in G$ and $(V_0 \subset V_1 \subset \cdots \subset V_n) \in \mathcal{F}$.

(v). Let $X = V^* := \text{Hom}(V, K)$ and let $\vartheta : G \to \mathfrak{S}(V^*)$ be defined by $\vartheta(g) := (g^{-1})^* = (g^*)^{-1}$ for $g \in G$.

**2).** Let $G$ be a group acting on a set $X$ with action homomorphism $\vartheta : G \to \mathfrak{S}(G)$ . We say that

(1) $G$ operates transitively on $X$ if $X/G$ is a singleton set, i.e. there is exactly one orbit.
(2) $G$ operates freely on $X$ if for every $x \in X$ the isotropy group $G_x$ at $x$ is trivial group, i.e. $G_x = \{e\}$.
(3) $G$ operates faithfully on $X$ if for every $g, h \in G$, $gx = hx$ for all $x \in X$ implies that $g = h$. Note that $G$ operates on $X$ faithfully if and only if the action homomorphism $\vartheta : G \to \mathfrak{S}(X)$ is injective.
(4) $G$ operates simply transitively on $X$ if $G$ operates transitively and freely on $X$.

**a).** For $x \in X$, the orbit $Gx$ of $x$ is invariant under $g$ for every $g \in G$ and so $G$ operates on $Gx$ transitively.

**b).** (Restriction of an action) Let $H$ be a subgroup of $G$. Then $H$ operates on $X$ by restriction; the corresponding action homomorphism is the composite homomorphism $H \xrightarrow{\iota} G \xrightarrow{\vartheta_X} \mathfrak{S}(X)$ .

**c).** (Left-translation action -- Cayley's representation) The binary operation of a group $G$ define a simple transitive operation on $G$. The corresponding action homomorphism is injective group homomorphism $\lambda : G \to \mathfrak{S}(G)$. This is the permutation representation of $G$ and is called the Cayley's representation of $G$. For any subgroup $H$ of $G$, the orbits of the restriction of the left-transaltion action to $H$ on $G$ are the right-cosets of $H$ in $G$ and the isotropy groups are trivial.

**d).** (Induced action) The normal subgroup $N = \ker \vartheta$ is called the kernel of the action of $G$ on $X$. Therefore $\vartheta$ induces a group homomorphism $\overline{\vartheta} : G/N \to \mathfrak{S}(X)$ and hence the quotient group $G/N$ acts on the set $X$ with the action homomorphism $\overline{\vartheta}$. This action of $G/N$ is called the induced action of $G$ on $X$. It is clear that $G/N$ acts faithfully on $X$.

**e).** The kernel of an operation of a group $G$ on a set $X$ is the intersection of all isotropy groups $G_x$, $x \in X$. – If $G$ is abelian, then $G$ operates simple trasitively if and only if $G$ operates transitively and faithfully.

**f).** If $\text{card}(G)$ is a prime number $>$ card $X$ then the action homomorphism is trivial, i.e., $\vartheta(g)(x) = x$ for every $g \in G$ and $x \in X$.

**g).** If $X$ is finite then the kernel of the action homomorphism $\vartheta$ is a subgroup of finite index in $G$.

**h).** Suppose that $G$ acts transitively on $X$ and $x \in X$. Then the map $G \to X$ defined by $g \mapsto g \cdot x$ is surjective and $\text{card}(X) = [G : G_x]$. In particular, if $G$ is finite then $X$ is finite and $\text{card}(X)$ divides $\text{card}(G)$.

**i).** The action homorphism $\vartheta : G \to \mathfrak{S}(X)$ induces many other operations, in a natural way. For example: (i). If $\psi : G' \to G$ is a homomorphism of groups, then the group $G'$ operates on $X$ by $g'x := \psi(g')x$, $g' \in G'$, $x \in X$. The corresponding group homomorphism of $G'$ in $\mathfrak{S}(X)$ is $\vartheta\psi$. (ii). If $\varphi : G \to G''$ is a surjective group homomorphism such that the kernel $\text{Ker}\,\varphi \subseteq \text{Ker}\,\vartheta$, then the group $G''$ operates on $X$ by $g''x := gx$, where $g \in \varphi^{-1}(g'')$ ia arbitrary. The corresponding group homomorphism $G'' \to \mathfrak{S}(X)$ is induced by $\vartheta : G \to \mathfrak{S}(X)$. (iii). If $X' \subseteq X$ is a $G$-invariant subset of $X$, i.e., for every $x \in X'$, the orbit $Gx$ of $x$ is contained in $X'$, then $G$ operates on $X'$ by restriction. In particular, $G$ operates on each orbit and in fact transitively.

**3).** (Class Equation) Let $G$ be a group operating on a set $X$. Then

$$\text{card}(X) = \text{card}(\text{Fix}_G(X) + \sum_{\substack{Gx \in X/G \\ \text{card}(Gx) > 1}} \text{card}(Gx).$$

**a).** (Class equation for the left-translation action --Lagrange's theorem) Let $G$ be a group and let $H$ be a subgroup. The group $H$ acts on $G$ by the restriction of the left-transaltion action of $G$ on $G$ to $H$; the orbits of this action are the right-cosets of $H$ in $G$ and the isotropy groups are trivial. Therefore the class equation for this action of $H$ on $G$ is $\text{card}(G) = \text{card}(H) \cdot \text{card}(G/H)$. In particular: (Lagrange's theorem) *Let $G$ be a finite group and let $H$ be a subgroup of $G$. Then the order of $H$ divides the order of $G$. More precisely,* $\text{ord}(G) = \text{ord}(H) \cdot [G : H]$.

**b).** (Conjugation action and the class equation for a group) Let $G$ be a group. Then $G$ acts on $G$ by the conjugate action, i.e. the action homomorphism is the group homomorphism $\kappa : G \to \text{Aut}(G)$, $g \mapsto \kappa_g : G \to G$, $x \mapsto gxg^{-1}$. The fixed point set of this operation is the center $\text{Z}(G)$ of $G$. The center of $G$ is also the kernel of this operation. In particular, the class equation for this operation is called the class equation for $G$ :

$$\text{card}(G) = \text{card}(Z(G)) + \sum_{j \in J} \text{card}(\text{C}_j),$$

where $\text{C}_j$, $j \in J$ are distinct conjugacy classes of $G$ with more than one element, i. e. $\text{C}_i \neq \text{C}_j$ for $i, j \in J$, $i \neq j$ and $\text{card}(\text{C}_j) > 1$ for every $j \in J$. If $x_i \in \text{C}_i$, then $\text{C}_i = \{gx_ig^{-1} \mid g \in G\}$ and $\text{card}(\text{C}_i) = [G : \text{Z}_G(x_i)]$, where for $x \in G$, $\text{Z}_G(x) := \{g \in G \mid gx = xg\}$ is the subgroup of elemenst of $G$ which commute with $x$. This subgroup is called the centraliser of $x$ in $G$. If $G$ is a finite group and $\text{C}_i$, $i = 1, \ldots, r$ are all distinct conjugacy classes in $G$ with $\text{card}(\text{C}_i) > 1$ for all $i = 1, \ldots, r$, then the numbers $\text{card}(\text{Z}(G))$ and $\text{card}(\text{C}_i)$, $i = 1, \ldots, r$ divide the order $\text{Ord}G$ of $G$ and the number of all conjugacy classes in $G$ is $\text{card}(\text{Z}(G)) + r$ and is called the class number of $G$.

**c).** Let $G$ be a finite group of odd order and let $x \in G$, $x \neq e$. Show that $\text{Z}_G(x) \neq \text{Z}_G(x^{-1})$, i.e. $x$ and $x^{-1}$ belongs to different conjugacy classes. (**Hint:** If $\text{Z}_G(x) = \text{Z}_G(x^{-1})$, then show that $\text{card}(\text{Z}_G(x))$ is even. But by b) $\text{card}(\text{Z}_G(x))$ divides the order $\text{ord}(G)$ of $G$ a contradiction. )

**d).** Let $p$ be a prime number and let $G$ be a finite group of order $p^n$ with $n \in \mathbb{N}^+$. Suppose that $G$ acts on a finite set $X$. Then $\text{card}(X) \equiv \text{card}(\text{Fix}_G(X)) \pmod{p}$. In particular, the center $\text{Z}(G)$ of $G$ is non-trivial. (**Hint:** For the last part use the class equation for $G$.)

**e).** Let $G$ be a finite group of order $n$ and let $p$ be a prime number. On the set $G^p$ of $p$-tuples of $G$ the cyclic group $H := \mathbb{Z}/\mathbb{Z}p$ operates by $\big(a, (x_1, \ldots, x_p)\big) \mapsto (x_{1+a}, \ldots, x_{p+a})$, where $a$ and the indices $1, \ldots, p$ are the residue classes in $\mathbb{Z}/\mathbb{Z}p$. The fixed points are the constant $p$-tuples $(x, \ldots, x)$. The group $\mathbb{Z}/\mathbb{Z}p$ also operates on the subset $X := \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdots x_p = e\}$ of $G^p$ (since $x_1x_2 \cdots x_p = (x_1 \cdots x_r)(x_{r+1} \cdots x_p) = e$ and so $(x_{r+1} \cdots x_p)(x_1 \cdots x_r) = e$ for $r = 1, \ldots, p-1$.) Therefore by part d) $\text{card}(X) = n^{p-1} \equiv |\text{Fix}_H\, X| \bmod p$.

(1) If $p$ divides $n$, then $p$ also divides $|\mathrm{Fix}_H X|$, i.e. *the cardinality of the set of $x \in G$ with $x^p = e$ is divisible by $p$.* In particular: (Cauchy's theorem) *Let $G$ be a finite group of order $n$ and let $p$ be a prime divisor of $n$. Then $G$ has an element of order $p$.* (2) If $p$ is not a divisor of $n$, then $\mathrm{Fix}_H X$ contain only the constant tuple $(e, \ldots, e)$. In particular: (Fermat's little theorem) *Let $p$ is a prime number and let $n \in \mathbb{N}^+$. If $p$ does not divide $n$, then $p$ divides $n^{p-1} - 1$, i.e. $n^{p-1} \equiv 1 \bmod p$.*

**f).** Let $p$ be a prime number. Then

(i). Every group of order $p^2$ is abelian and in fact either a cyclic or isomorphic to a product of two cyclic groups of order $p$. (**Hint**: Use 3)-c)). )

(ii). Every group of order $2p$ is either cyclic or isomorphic to the Dihedral group $\mathrm{D}_p$. (**Remark**: For Dihedral groups see Exercise T8.???. The case $p = 2$ is a special case. )

(iii). Let $G$ be a non-abelian group of order $p^3$. Show that the derived subgroup (the subgroup of $G$ generated by the set of all commutators $\{[a, b] \mid aba^{-1}b^{-1} \mid a, b \in G\}) = [G, G] = \mathrm{Z}(G)$ and the class number of $G$ is $p^2 + p - 1$. (**Hint**: $G$ acts transitively on $G \setminus \{e\}$ by the conjugation action. Then use 2)-h). — **Remark** There exists infinite groups of class number 2. For class numbers see 3)-b).)

(iv). Compute the class number of the group $\mathfrak{S}_n$ for $n \leq 6$.

**4).** Let $G$ and $H$ be two groups acting on the sets $X$ and $Y$ with action homomorphisms $\vartheta_X : G \to \mathfrak{S}(X)$ and $\vartheta_Y : H \to \mathfrak{S}(Y)$ respectively.

**a).** (Product action) The product group $G \times H$ acts on the product set $X \times Y$ with the action homomorphism $\vartheta_{X\times Y} : G \times H \to \mathfrak{S}(X \times Y)$ defined by $(g, h) \mapsto \vartheta_X(g) \times \vartheta_Y(h)$ for $g \in G$ and $h \in H$. This action is called the product action of $G \times H$ on $X \times Y$. The orbit $(G \times H)(x, y)$ of $(x, y) \in X \times Y$, is the product $G \cdot x \times H \cdot y$ of orbtis of $x$ and $y$. What is the isotropy subgroup $(G \times H)_{(x,y)}$ at $(x, y)$ ?

**b).** (Diagonal action) Suppose that $H = G$ above. Then the group $G$ acts on $X \times Y$ with the action homomorphism $G \xrightarrow{\Delta_G} G \times G \xrightarrow{\vartheta_{X\times Y}} \mathfrak{S}(X \times Y)$, where $\Delta_G : G \to G \times G$ is the diagonal homomorphism defined by $g \mapsto (g, g)$ for $g \in G$ and $\vartheta_{X\times Y}$ is defined as above with $H = G$. This action is called the diagonal action of $G$ on $X \times Y$. The isotropy subgroup $G_{(x,y)}$ of $(x, y) \in X \times Y$ is the intersection $G_x \cap G_y$ of the isotropy subgroups of $x$ and $y$. What is the orbit $G(x, y)$ of $(x, y)$?

**c).** Give an example to show that the diagonal action of $G$ on $X \times Y$ need not be transitive even if $G$ acts transitively on both $X$ and $Y$. (**Hint**: Take the left translation action (see 2)-c)) of $G$ on $X = Y = G$. )

**5).** (Automorphism actions) Let $G$ and $H$ be two groups. Suppose that the group $G$ acts on $H$ with the action homomorphism $\vartheta : G \to \mathfrak{S}(H)$. If $\mathrm{im}(\vartheta) \subseteq \mathrm{Aut}(H) =$ (the set of all automorphisms of the group $H$) then we say that $G$ acts on $H$ by automorphisms or $\vartheta$ is an automorphism action and in this case we write $\vartheta : G \to \mathrm{Aut}(H)$ instead of $\vartheta : G \to \mathfrak{S}(H)$.

**a).** The automorphism group $\mathrm{Aut}(G)$ of $G$ acts on $G$ in a natural way, infact by automorphisms; the automorphism action $\vartheta = \mathrm{id}_{\mathrm{Aut}(G)} : \mathrm{Aut}(G) \to \mathrm{Aut}(G)$. The subset $G \setminus \{e\}$ is invariant under this action.

**b).** The conjugate action of the group $G$ on $G$ is the automorphism action $\kappa : G \to \mathrm{Aut}(G)$, $g \mapsto \kappa_g$, where for $g \in G$, $\kappa_g : G \to G$ is the inner automorphism of $G$ defined by $x \mapsto gxg^{-1}$ for $x \in G$. What is the kernal of this action ?

**c).** Let $N$ be an (additive) abelian group. The cyclic group $\mathbb{Z}^\times = \{1, -1\}$ of order 2 operates on $N$ by automorphisms, where $-1$ operates as the inverse map $x \mapsto -x$ of the group $N$.

**6).** ($k$-transitive actions) Let $G$ be a group and let $X$ be a $G$-set with the action homomorphism $\vartheta : G \to \mathfrak{S}(X)$. Let $k \in \mathbb{N}^+$. Then $X$ is called $k$-transitive or we say that $G$ acts $k$-transitively on $X$ if for any two $k$-tuples $(x_1, \ldots, x_k) \in X^k$ with $x_i \neq x_j$ for $1 \leq i \neq j \leq k$ and $(y_1, \ldots, y_k) \in X^k$ with $y_i \neq y_j$ for $1 \leq i \neq j \leq k$, there exists an element $g \in G$ such that $\vartheta(g)(x_i) = y_i$ for every $1 \leq i \leq k$. 1-transitive is same as transitive (see 2)-(1)).

**a).** Let $k \in \mathbb{N}^+$. If $\mathrm{card}(X) < k$ then $X$ is $k$-transitive vacuously. If $\mathrm{card}(X) \geq k$ and $X$ is $k$-transitive then $X$ is $r$-transitive for every $1 \leq r \leq k$.

**b).** For $n \in \mathbb{N}^+$, any subgroup of $\mathfrak{S}_n$ acts naturally on the set $\{1, \ldots, n\}$, in fact, the action homomorphism is tha natural inclusion $\iota : G \to \mathfrak{S}_n$. This natural action of the permutation group $\mathfrak{S}_n$ (respectively, the *alternating group* $\mathfrak{A}_n$) on the set $\{1, \ldots, n\}$ is $n$-transtive (respectively, $(n-2)$-transitive but not $(n-1)$-transitive).

**c).** The subset $X^{(n)} := \{(x_1, \ldots, x_n) \mid x_i \in X, x_i \neq x_j, 1 \leq i \neq j \leq n\}$, $(n \in \mathbb{N}^+)$ of $X^n$ is a $G$-subset of the diagonal action (see 4)-b)) of $G$ on $X^n$. Then $G$ acts $n$-transitively on $X$ if and only if $G$-acts transitively on $X^{(n)}$.

**d).** The isotropy subgroup $G_x$, $x \in X$ acts on $X \setminus \{x\}$ in a natural way. If $G$ acts transtively on $X$, then $G$ acts 2-transitively on $X$ if and only if $G_x$ transitively on $X \setminus \{x\}$ for every $x \in X$.

**e).** If $G$ is a finite group, $G$ acts 2-transitively on $X$ and $[G : G_x] = n$ for $x \in X$, then $(n-1)n$ divides $\mathrm{ord}(G)$. (**Hint:** Use 2)-g). )

**7).** (Left coset $G$-sets) Let $G$ be any group and let $H$ be a subgroup of $G$. Let $X := G/H = \{xH \mid x \in G\}$ be the set of all left cosets of $H$ in $G$ and let $\vartheta : G \to \mathfrak{S}(G/H)$ be defined by $\vartheta(g) := \widetilde{g} : G/H \to G/H, xH \mapsto gxH$ for $xH \in G/H$. Then $X = G/H$ is a $G$-set with the action homomorphism $\vartheta$. This $G$-set is called the left coset $G$-set of $H$ in $G$.

**a).** $G$ acts transitively on $G/H$ and the isotropy group at $H$ is $G_H = H$. In particular, the isotropy subgroups are $gHg^{-1}$, $g \in G$ and so $N = \cap_{g \in G} gHg^{-1}$ is the kernel of the action of $G$ on $G/H$. Therefore $G/N$ acts faithfully on $G/H$ with the induced action homomorphism $\overline{\vartheta} : G/N \to \mathfrak{S}(G/H)$. Further, $N$ is the biggest normal subgroup of $G$ contained in $H$ and the quotient group $G/N$ is isomorphic to a subgroup of the permutation group of $G/H$. (**Hint:** Let $F$ be a normal subgroup of $G$ with $F \subseteq H$. Then $F = gFg^{-1} \subseteq gHg^{-1}$ for every $g \in G$. Therefore $F \subseteq \cap_{g \in G} gHg^{-1} = N$ )

**b).** If $[G : H]$ is finite then so is $[G : N]$ and $[G : N]$ divides $[G : H]!$. (**Hint:** Follows from part a) that $\overline{\vartheta} : G/N \to \mathfrak{S}(G/H)$ is injective. )

**8).** ($G$-homomorphisms) Let $G$ be a group and let $X$, $Y$ be two $G$-sets with the operation maps $\varphi_X : G \times X \to X$ and $\varphi_Y : G \times Y \to Y$ respectively. A map $f : X \to Y$ is called a $G$-homomorphism if $f(gx) = gf(x)$ for every $g \in G$ and $x \in X$, i.e. the diagram

$$\begin{array}{ccc} G \times X & \xrightarrow{\varphi_X} & X \\ {\scriptstyle \mathrm{id} \times f}\downarrow & & \downarrow{\scriptstyle f} \\ G \times Y & \xrightarrow{\varphi_Y} & Y \end{array}$$

is commutative. A $G$-homomorphism $f : X \to Y$ is called a $G$-isomorphism if there exists a $G$-homomorphism $f' : Y \to X$ such that $f' \circ f = \mathrm{id}_X$ and $f \circ f' = \mathrm{id}_Y$.

Let $f : X \to Y$ be a $G$-homomorphism. Then

**a).** The orbit $Gx$ is mapped onto the orbit $Gf(x)$ for every $x \in X$; in particular, induces a map $\overline{f} : X \backslash G \to Y \backslash G$ on the quotient spaces such that the diagramm

$$\begin{array}{ccc} X & \longrightarrow & X/G \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \overline{f}} \\ Y & \longrightarrow & Y/G \end{array}$$

is commutative, where $X \to X/G$ and $Y \to Y/G$ are the cannonical projection maps.

**b).** $f(\mathrm{Fix}_G(X)) \subseteq \mathrm{Fix}_G(Y)$. In particular, $f$ induces a mapping $\mathrm{Fix}_G(X) \to \mathrm{Fix}_G(Y)$.

**c).** For $x \in X$, the isotropy subgroup $G_x$ is a subgroup of $G_{f(x)}$.

**d).** $f$ is a $G$-isomorphism if and only if $f$ is bijective. Moreover, in this case, the diagram

$$\begin{array}{ccc} G & \xrightarrow{\vartheta_X} & \mathfrak{S}(X) \\ \| & & \downarrow{\scriptstyle \Phi_f} \\ G & \xrightarrow{\vartheta_Y} & \mathfrak{S}(Y) \end{array}$$

of groups and group homomorphisms is commutative, where $\vartheta_X$, $\vartheta_Y$ are action homomorphisms of $X$, $Y$ respectively and $\Phi_f : \mathfrak{S}(X) \to \mathfrak{S}(Y)$ is the group homomorphism defined by $\Phi_f(\sigma) := f \circ \sigma \circ f^{-1}$ for $\sigma \in \mathfrak{S}(X)$.

**e).** More generally, let $\varphi : G \to H$ be a homomorphism of groups. Suppose that $G$ and $H$ operates on the sets $X$ and $Y$ respectively. A map $f : X \to Y$ is called $\varphi$-invariant map if for all $g \in G$ and for all $x \in X$, we have : $f(gx) = \varphi(g) f(x)$, i.e. if the canonical diagramm

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ {\scriptstyle \varphi \times f}\downarrow & & \downarrow{\scriptstyle f} \\ H \times Y & \longrightarrow & Y \end{array}$$

is commutative. A map $f : X \to Y$ $\varphi$-invariant if and only if $f$ is a $G$-invariant map, where the $H$-operation on $Y$ via $\varphi$ defines a $G$-operation on $Y$, i.e. $gy := \varphi(g)y$, $g \in G$, $y \in Y$.

**9).** Let $G$ be a group acting on a set $X$ with the corresponding group homorphism $\vartheta : G \to \mathfrak{S}(X)$. This homomorphism induces many other operations, in a natural way. For example:

**a).** A map $f : X \to Y$ is said to be compatible with the operation of $G$ on $X$ if for all $x, x' \in X$, the equality $f(x) = f(x')$ implies the equality $f(gx) = f(gx')$ for all $g \in G$. Moreover, if $f$ is surjective, then the operation of $G$ on $X$ induces an operation of $G$ on $Y$ by $gy := f(gx)$, where $x \in f^{-1}(y)$ is arbitrary. This mean that the map $f$ is a $G$-map. Further, in this case $f(\mathrm{Fix}_G(X)) \subseteq \mathrm{Fix}_G(Y)$. Give an example to show that this inclusion can be strict. (**Hint :** Let $G$ be the multiplicative cyclic group $\{-1, 1\}$ of order 2, $X := \mathbb{Z}$ and $Y := \mathbb{Z}_2 = \{0, 1\}$. Then $G$ acts on $X$ (resp. on $Y$) by the action homomorphism $\vartheta : G \to \mathrm{Aut}\,\mathbb{Z}$ (resp. $\vartheta : G \to \mathrm{Aut}\,\mathbb{Z}_2$), $\vartheta(1) = \mathrm{id}_{\mathbb{Z}}$ and $\vartheta(-1) : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto -n$ (resp. $\vartheta(1) = \mathrm{id}_{\mathbb{Z}_2}$ and $\vartheta(-1) : \mathbb{Z}_2 \to \mathbb{Z}_2$, $n \mapsto -n$). Further, let $f : \mathbb{Z} \to \mathbb{Z}_2$ be the canonical surjective map. Then $\mathrm{Fix}_G(X) = 0$ and $\mathrm{Fix}_G(Y) = Y$. )

**b).** Let $Y$ be an another set. Then $G$ operates on the set of all maps $X^Y$ by $(g\widetilde{f})(y) := g\big(\widetilde{f}(y)\big)$, $g \in G$, $\widetilde{f} \in X^Y$ and $y \in Y$. The action homomorphism of the $G$-set $X^Y$ is $\lambda_X^Y \circ \vartheta : G \to \mathfrak{S}(X) \to \mathfrak{S}(X^Y)$, where $\lambda_X^Y$ is defined in the footnote [2]) below and the fixed set $\mathrm{Fix}_G(X^Y) = \{f \in X^Y \mid \mathrm{im}(f) \subseteq \mathrm{Fix}_G(X)\}$. The map $c : X \to X^Y$ defined by $x \mapsto c_x : Y \to X =$ the constant map $y \mapsto x$, is a $G$-homomorphism.

**c).** Let $Y$ be an another set. Then $G$ operates on the set of all maps $Y^X$ by $(gf)(x) := f(g^{-1} \cdot x)$, $g \in G$, $f \in Y^X$ and $x \in X$. The action homomorphism of the $G$-set $Y^X$ is $\rho_X^Y \circ \vartheta : G \to \mathfrak{S}(X) \to \mathfrak{S}(Y^X)$, where $\rho_X^Y$ is defined in the footnote [2]) below and the fixed set $\mathrm{Fix}_G(Y^X) = \{f \in X^Y \mid f \text{ is constant on the } G\text{-orbits of } X\}$.

**d).** Let $H$ be an another group and let $Y$ be a $H$-set. Then the product group $H \times G$ operates on the set $Y^X$ by $((h, g)f)(x) := h \cdot f(g^{-1} \cdot x)$, $(h, g) \in H \times G$, $f \in Y^X$ and $x \in X$. The action homomorphism of the $H \times G$-set $Y^X$ is $\vartheta_Y \times \vartheta_X \circ \mu_{YX} : H \times G \to \mathfrak{S}(Y) \times \mathfrak{S}(X) \to \mathfrak{S}(Y^X)$, where $\mu_{YX}$ is defined in the footnote [2]) below. In particular, if $H = G$ and if $Y$ is a $G$-set then the set $Y^X$ is a $G \times G$-set and so $G$ acts on $Y^X$ via the diagonal homomorphism $G \to G \times G$, $g \mapsto (g, g)$, $g \in G$. the fixed set $\mathrm{Fix}_G(Y^X) = \mathrm{Hom}_G(X, Y) = \{f \in Y^X \mid f \text{ is a } G\text{-homomorphism}\}$.

**10).** Let $G$ be a group and let $H$ be a subgroup of $G$.

**a).** If $H$ is of finite index in $G$, then $H$ contains a normal subgroup $N$ of finite index such that $[G : N]$ divides $[G : H]!$.

**b).** If $G$ is simple and $H \neq G$, then $G$ isomorphic to a subgroup of $\mathfrak{S}(G/H)$. In particular, if $G$ is simple and $H$ is a subgroup of $G$ of finte index $n > 1$, then $G$ is finite, moreover, order of $G$ divides $n!$. (**Hint :** Look at the kernel of the action of the left-coset $G$-set $G/H$ (see 7)). )

**c).** $H$ is normal in $G$ if and only if the orbits of the restriction action of $H$ on the left-coset $G$- set $G/H$ are singleton.

---

[2]) **Set Theoretic Results** Let $X$ and $Y$ be two sets. For $\sigma \in \mathfrak{S}(X)$, let $\lambda_\sigma : X^Y \to X^Y$ (resp. $\rho_\sigma : Y^X \to Y^X$) be defined by $f \mapsto \sigma \circ f$ for $f \in X^Y$ (resp. $f \mapsto f \circ \sigma$ for $f \in Y^X$). For $(\tau, \sigma) \in \mathfrak{S}(Y) \times \mathfrak{S}(X)$, let $\mu_{(\tau,\sigma)} : Y^X \to Y^X$ be defined by $f \mapsto \tau \circ f \circ \sigma$ for $f \in Y^X$. Show that the maps

(i) $\lambda_X^Y : \mathfrak{S}(X) \to \mathfrak{S}(X^Y)$ defined by $\sigma \mapsto \lambda_\sigma$

(ii) $\rho_X^Y : \mathfrak{S}(X) \to \mathfrak{S}(Y^X)$ defined by $\sigma \mapsto \rho_\sigma$

(iii) $\mu_{YX} : \mathfrak{S}(Y) \times \mathfrak{S}(X) \to \mathfrak{S}(Y^X)$ defined by $(\tau, \sigma) \mapsto \mu_{(\tau,\sigma)}$

are group homomorphisms.

**d).** (Yang) If $G$ is finite and $H$ is a subgroup of prime index $p$, where $p$ is the smallest prime divisor of Ord $G$, then $H$ is normal in $G$. In particular, if every subgroup of a group $G$ of order $p^n$, $n \in \mathbb{N}^+$ of index $p$ is normal in $G$.

**e).** Suppose that $G$ is finite and $\text{ord}(G) = mn$, $\text{ord}(H) = n$.

(i). Let $N$ be the kernel of the action of the left coset $G$-set $G/H$. Then $[H : N]$ divides $\gcd(n, (m-1)!)$. (ii). (Frobenius) If $n$ has no prime factor less than $m$ then $H$ is normal in $G$. (**Hint:** Use (i) above. ) (iii). If $\text{ord}(G) = 2^r \cdot 3$ with $r \in \mathbb{N}^+$, then $G$ has a normal subgroup of order $2^r$ or $2^{r-1}$. In particular, if $r \geq 2$ then $G$ is not simple. (**Hint:** Apply (1) above to the 2-Sylow subgroup $H$ of $G$.)

**f).** If $H$ is normal in $G$ then the orbits of the restriction of any transitive $G$-action to $H$ have the same cardinality. (**Hint:** Let $X$ be a transitive $G$-set. For $g \in G$ and $x \in X$, the maps $Hx \to g^{-1}Hgx$, $hx \mapsto g^{-1}hgx$ and $g^{-1}Hgx \to Hgx$, $g^{-1}hgx \mapsto hgx$ are bijective. )

**g).** The product group $H \times H$ acts on $G$ with the action homomorphism $\vartheta : H \times H \to G$ defined by $\vartheta(h', h)(x) = h'xh^{-1}$, for $(h', h) \in H \times H$ and $x \in G$. Then $H$ is normal in $G$ if and only if every orbit of the action defined by $\vartheta$ has the cardinality $= \text{card}(H)$.

**11).** Let $G$ be a group. Then $G$ operates on the power-set $\mathfrak{P}(G)$ of $G$ by conjugation. For a subset $A$ of $G$ the isotropy group $G_A$ with respect to this operation is called the normaliser of $A$ in $G$ and is denoted by $\text{N}_G(A)$.

**a).** The subgroup $\text{N}_G(A)$ is the biggest subgroup of $G$, which operates on $A$ by conjugation.

**b).** The kernel of this operation of $\text{N}_G(A)$ on $A$ is the centraliser $\text{Z}_G(A) = \bigcap_{a \in A} \text{Z}_G(a)$ of $A$. In particular, $\text{Z}_G(A)$ is normal in $\text{N}_G(A)$.

**c).** If $H$ is a subgroup of $G$, then $\text{N}_G(H)$ is the biggest subgroup of $G$ in which $H$ is normal.

**d).** The index $[G : \text{N}_G(H)]$ is the number of conjugate subgroups of $H$ in $G$ and if $[G : H]$ is finite, then $[G : \text{N}_G(H)]$ divides $[G : H]$.

**12).** Let $G$ and $H$ be finite groups. Then

**a).** The order of $G$ is a power of a prime number $p$ if and only if order of every element of $G$ is a power of $p$. (**Hint:** Use Cauchy's theorem 3)-d)(1)). — **Remark:** A group in which order of every element $G$ is a power of a prime number $p$, is called a $p$-group.)

**b).** Every subgroup of the product group $G \times H$ is of the form $G' \times H'$, where $G'$ is a subgroup of $G$ and $H'$ is a subgroup of $H$ if and only if the orders of $G$ and $H$ are relatively prime. (**Hint:** Use Cauchy's theorem 3)-d)(1)). )

**13).** Let $X$ be a $G$-set. A subset $Y$ of $X$ is called a $G$-subset if $gy \in Y$ for every $g \in G$ and $y \in Y$. If $Y \subseteq X$ is a $G$-subset of $X$ then the natural inclusion map $Y \hookrightarrow X$ is a $G$-homomorphism. Each orbit of $X$ under $G$ is a transitive $G$-subset of $X$.

**a).** Every subset $Y$ of a $G$-set $X$ is a $G$-subset if and only if it is a union of orbits of $X$ under $G$. Moreover, if $Y$ is transitive $G$-subset of $X$ then $Y$ must be an orbit of $x \in X$ under $G$.

**b).** Let $\{X_i \mid i \in I\}$ be a collection of $G$-sets.

(1) If $X_i$ are disjoint, that is, $X_i \cap X_j = \emptyset$ for every $i, j \in I$ with $i \neq j$ then show that $\cup_{i \in I} X_i$ is a $G$-set in a natural way.
(2) If $X_i$ are not necessarily disjoint then $X_i' := \{(x, i) \mid x \in X_i, i \in I\}$ are disjoint and each $X_i'$ is a $G$-set in a natural way. Further the maps $X_i \to X_i'$ defined by $x \mapsto (x, i)$ are $G$-isomorphisms.

**c).** Suppose that $X$ is a transitive $G$-set and Let $x_0 \in X$ and let $Y$ be the left coset $G$-set of the isotropy subgroup $G_{x_0}$, i.e. $Y = G/G_{x_0}$ with the natural (see 7)) $G$-action on $Y$. Show that there exists a $G$-isomorphism $f : X \to Y$. (**Hint:** For $x \in X$, let $g \in G$ with $gx_0 = x_0$ and put $f(x) := gG_{x_0}$. )

**d).** Every $G$-set $X$ is isomorphic to the disjoint union of left coset $G$-sets. (**Hint:** $X$ is the disjoint union of its orbits which are transitive $G$-subsets of $X$. Now use the parts c) and b)-1) above. )

**14).** Let $G$ be a subgroup of $\mathfrak{S}_n$, $n \geq 2$. Suppose that the natural operation of $G$ on $\{1, \ldots, n\}$ is transitive.

**a).** If $G$ contain a transposition and a cycle of order $n-1$, then $G = \mathfrak{S}_n$. (**Hint:** Use T8.1-4)-l)-a). )

**b).** If $G$ contain a transposition and a cycle of prime order $p$ with $\frac{n}{2} < p < n$, then $G = \mathfrak{S}_n$.

**15).** Let $p$ be a prime number.

**a).** If the subgroup $G$ of $\mathfrak{S}_p$ contain a transposition and if $p$ divides the order of $G$, then $G = \mathfrak{S}_p$. (**Hint:** $G$ contain an element of order $p$. This must be a cycle. Now use T8.1-4)-l)-c). — **Remark:** Show that the condition "$p \mid |G|$" is equivalent with "the natural opeartion of $G$ on $\{1, \ldots, p\}$ is transitive".)

**b).** Let $G$ be the subgroup of $\mathfrak{S}_{p+1}$. Suppose that $G$ has the following properties:
(1) The natural opeartion of $G$ on $\{1, \ldots, p+1\}$ is transitive.
(2) $p$ divides the order of $G$.
(3) $G$ contains a transposition.
Then $G = \mathfrak{S}_{p+1}$. (**Hint:** Use 14)-a).)

**16).** Let $G$ be a finitely generated group and let $n \in \mathbb{N}^+$.

**a).** The set of all subgroups of index $n$ in $G$ is finite. (**Hint:** Using left coset $G$-sets reduce the problem to that of normal subgroups and these are nothing but kernels of the group homomorphisms $G \to \mathfrak{S}_n$ which are finitely many. Why ? )

**b).** Let $\varphi : G \to G$ be a surjective endomorphism of $G$. Show that the mapping $H \mapsto \varphi^{-1}(H)$ is a bijection on the set of all subgroups of index $n$ in $G$. (**Hint:** Use the part a) above. )

**17).** A group $G$ is called homogeneous if the natural action (see 5)) of the automorphism group $\mathrm{Aut}(G)$ of $G$ on $G$ is transitive on the $\mathrm{Aut}(G)$-subset $G \setminus \{e\}$. Show that if $G$ is a finite group then $G$ is homogeneous if and only if $G$ is a finite product of $\mathbb{Z}_p = \{0, \ldots, p-1\}$ = the cyclic group of prime order $p$.

**18).** Let $H$ be a subgroup of finite index in a group $G$. If $G = \bigcup_{g \in G} gHg^{-1}$ then show that $G = H$.(**Hint:** Let $N$ be the kernel of the action of the left coset $G$-set $G/H$. By passing to the group $G/N$ reduce to the case of finite groups. – or use 11).). Give an example to show that the assumption finite index is necessary. (**Hint:** $H = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in G \mid ac \neq 0 \right\} \neq G = \mathrm{GL}(2, \mathbb{C}) = \bigcup_{g \in G} gHg^{-1}$. )

**19).** (Semi-direct Product – Holomorph of a group) Let $N$ and $H$ be groups. Suppose that $H$ operates on $N$ by automorphisms (see 5)), i.e. the action homomorphism is $\vartheta : H \to \mathrm{Aut}\, N \subseteq \mathfrak{S}(N)$. We shall construct a group $G$ such that $H$ is a subgroup of $G$ and $N$ is a normal subgoup of $G$ and the given operation of $H$ on $N$ is the conjugation of $H$ on $N$. Let $G := N \times H$ and define the multiplication in $G$ by $(n, h)\,(n', h') := (n\, \vartheta_h(n')\,, hh')$. (**Hint:** The group axioms for $G$ can be easily verified; the element $(e_N\,, e_H)$ is the identity element and the inverse of $(n, h)$ is $(\vartheta_{h^{-1}}(n^{-1})\,, h^{-1})$. The group $N$ can be identified with the normal subgroup $N \times \{e_H\}$ of $G$ and the group $H$ can be identified with the subgroup $\{e_N\} \times H$ of $G$. With this identification the pair $(n, h)$ is the product $nh = (n, e_H)(e_N, h)$. )This group $G$ is called the semi-direct product of the groups $N$ and $H$ with respect to the operation $\vartheta$ of $H$ on $N$. The semi-direct product of $N$ and $H$ with respt to $\vartheta : H \to \mathrm{Aut}\, N$ is denoted by $N \rtimes H = N \rtimes_\vartheta H$.

**a).** The operation $\vartheta$ of $H$ on $N$ is trivial if and only if $G = N \rtimes H$ is the product group. This can also be characterised by the condition that $H$ is normal in $G$.

**b).** Suppose that $H = \mathrm{Aut}\, N$ and $\vartheta$ is the natural action (see N11.6-a)) on $N$. Then the corresponding semi-direct product is called the full holomorph of $N$ and is denoted by $\mathrm{Hol}\, N$. In the case $H \subseteq \mathrm{Aut}\, N$ is a subgroup, the semi-direct product is called a holomorph of $N$.

**c).** The full holomorph (and hence every holomorph) of $N$ can be canonically embedded in the permutation group $\mathfrak{S}(N)$ of $N$, where the normal subgroup $N$ of $\mathrm{Hol}\,(N)$ is identified with the group of left-translations of $N$ using the Cayley's representation and $\mathrm{Aut}\, N$ is embedded canonically in $\mathfrak{S}(N)$, i.e. the map $(n, \sigma) \mapsto \lambda_n \sigma$, $n \in N$, $\sigma \in \mathrm{Aut}\, N$ is an injective group homomorphism of $\mathrm{Hol}\,(N)$ into the permutation group $\mathfrak{S}(N)$, where $\lambda_n$ for $n \in N$ denote the left-translation by $n$.

**d).** The subgroup $\mathrm{Hol}\,(N)$ of $\mathfrak{S}(N)$ is generated by the left-translations and the automorphisms of $N$. Further, since $\rho_n = \lambda_n \circ \kappa_{n^{-1}} = \kappa_{n^{-1}} \circ \lambda_n$ for $n \in N$, the subgroup $\mathrm{Hol}\,(N)$ also contain right-translationen.

**20).** (Dihedral groups) Let $N$ be an (additive) abelian group. The cyclic group $\mathbb{Z}^\times = \{1, -1\}$ of order 2 operates on $N$ by automorphisms (see 5)), where $-1$ operates as the inverse map $x \mapsto -x$

of the group $N$. The corresponding semi-direct product is called the dihedral group of $N$ and is denoted by $\mathbf{D}(N)$. The binary operation in $\mathbf{D}(N)$ is given by $(n, \varepsilon)\,(n', \varepsilon') = (n + \varepsilon n', \varepsilon\varepsilon')\,,\ n, n' \in N$, $\varepsilon, \varepsilon' \in \mathbb{Z}^\times$.

**a).** The dihedral group $\mathbf{D}(N)$ is the direct product of $N$ and $\mathbb{Z}^\times$, i.e. is an abelain group if and only if the inverse map of $N$ is trivial, i.e. every element of $N$ is its inverse in $N$. [3])

**b).** If $N = \mathbf{Z}_n = \mathbb{Z}/\mathbb{Z}n$ is the cyclic group of order $n > 0$, then for $\mathbf{D}(N)$ we simply write $\mathbf{D}_n$; its order is $\operatorname{Ord}\mathbf{D}_n = 2n$. The infinite dihedral group $\mathbf{D}_0 := \mathbf{D}(\mathbb{Z})$ is the full holomorph of the additive group $\mathbb{Z}$. Therefore we have a sequence $\mathbf{D}_n$, $n \in \mathbb{N}$, of the dihedral groups. (**Remark:** We shall show that the dihedral group $\mathbf{D}(\mathbb{R})$ is isomorphic to the group of motions of an affine Euclidean line and the dihedral group $\mathbf{D}\,(\mathbb{R}/\mathbb{Z})$ is isomorphic to the group of isometries of an (oriented) two-dimensional Euclidean vector space. The group $\mathbf{D}(\mathbb{R}/\mathbb{Z})$ (and occasionally the group $\mathbf{D}(\mathbb{Q}/\mathbb{Z})$ ) is also denoted by $\mathbf{D}_\infty$ .

**21).** Let $N$ be a group. Then every semi-direct product (see 19)) of the form $N \rtimes H$, where $H$ is a group, is equal to the direct product $N \times H$ if and only if $N$ has at most two elements. (**Hint:** It is enough to show that *every group $N$ with more than two elements has an automorphism different from the identity map.* – In the non-abelian case the conjugation, and in the abelain case the inverse map and for the elementary abelian 2-groups, see footnote 1, the linear map of $\mathbf{K}_2$-vector spaces. — This result can also be formulated as: Every weak-split exact sequence of groups $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is strong-split if and only if $N$ has atmost two elements. )

**22).** Suppose that a finite group $G$ of order $n$ operates on the (additively written) abelian group $H$ as a group of automorphisms.

**a).** $\operatorname{Fix}_G H$ is a subgroup of $H$.

**b).** For every $x \in H$, the sum $\mathrm{N}x := \sum_{g\in G} gx$ is a fixed point of the operation of $G$. (**Hint:** $h\,(\mathrm{N}x) = \sum_{g\in G}(hg)x = \sum_{g\in G} gx = \mathrm{N}x$ for every $h \in G$, since $G = \{hg \mid g \in G\}$.)

**c).** (Mean) Suppose that the multiplication $\lambda_n$ by $n$ on $H$ is bijektive. Then $\lambda_n$ and the inverse $(\lambda_n)^{-1}$ of $\lambda_n$ are $G$-invariant. The element $\pi_H x := \frac{1}{n}\,\mathrm{N}x = \frac{1}{n}\sum_{g\in G} gx$ is called the mean or average of $x$ and is fixed point.

**d).** The group homomorphism $\pi_H : H \to H$ is a projection of $H$ onto the subgroups $\operatorname{Fix}_G H$, i.e. $\pi_H = \pi_H^2$ and $\operatorname{im}\pi_H = \operatorname{Fix}_G H$. (**Hint:** Let $\pi := \pi_H$. The inclusion $\pi(H) \subseteq \operatorname{Fix}_G H$ is mentioned in the part b). Conversely, let $x \in \operatorname{Fix}_G H$, then $\pi x = \frac{1}{n}\sum_{g\in G} gx = \frac{1}{n}nx = x$. This proves the inclusion $\operatorname{Fix}_G H \subseteq \pi(H)$ and hence $\pi = \pi^2$. — **Remark:** This is the most effective way of computing the fixed points. For example, it can be applied to the additive group $H$ of a vector space over a field $K$ with $n \cdot 1_K \neq 0$ (or moregenerally to the additive groups of a module over a ring $A$ with $n \cdot 1_A \in A^\times$). )

**e).** Let $G$ be a finite group of order $n$ and let $H', H$ resp. $H''$ be abelain groups on which $G$ operates by automorphisms. Further, let $H' \xrightarrow{f'} H \xrightarrow{f} H''$ be an exact sequence of $G$-invariant group homomorphisms. If the multiplication by $n$ on $H$ and $H'$ are bijective [4]), then the induced sequence $\operatorname{Fix}_G H' \to \operatorname{Fix}_G H \to \operatorname{Fix}_G H''$ is also exact. (**Hint:** For $x \in \operatorname{Fix}_G H$ with $f(x) = 0$ we need to find $x' \in \operatorname{Fix}_G H'$ with $f'(x') = x$. Let $\widetilde{x} \in H'$ be such that $f'(\widetilde{x}) = x$. Then $x' := \pi'_H(\widetilde{x}) \in \operatorname{Fix}_G H'$ and $f'(x') = f'\pi'_H(\widetilde{x}) = \pi_H f'(\widetilde{x}) = \pi_H x = x$ . — **Remark:** In the above situation, the sequence of the fixed-point groups is not exact in general, for example, the group $G := \mathbb{Z}^\times = \{1, -1\}$ operates (see 5)-c)) in a natural way, i.e. the operation of $-1$ is the inverse map. Then the canonical projection of $\mathbb{Z}$ onto $\mathbb{Z}/\mathbb{Z}2$ is surjective, but the induced homomorphism $0 \to \mathbb{Z}/\mathbb{Z}2$ on the fixed-point groups is not surjective. )

**23).** Let $G$ be a finite group of order $n$. Then $G$ acts on the power set $\mathfrak{P}(G)$ of $G$ by the left-multiplication, i.e. the action homomorphism is $\vartheta : G \to \mathfrak{S}(\mathfrak{P}(G))$ given by $g \mapsto \vartheta(g)$, where $\vartheta(g) : \mathfrak{P}(G) \to \mathfrak{P}(G)$ is defined by $A \mapsto gA := \{ga \mid a \in A\}$.

---

[3]) Such a group $N$ is called an elementary (abelian) 2-group. They are precisely the additive groups of the vector spaces over the field $\mathbf{K}_2$ with 2 elements.

[4]) It is enough to assume that on $H'$ it is surjective and on $\operatorname{im} f' = \operatorname{Ker} f$ it is injective.

**a).** For every fixed positive integer $r \leq n$, the subset $\mathfrak{P}_r(G) := \{A \in \mathfrak{P}(G) \mid \mathrm{card}(A) = r\}$ of a $G$-set $\mathfrak{P}(G)$ is invariant under the above $G$-action.

**b).** Each orbit of $\mathfrak{P}(G)$ under the above $G$-action contains either exactly one subgroup of $G$ or contains no subgroup of $G$. (**Proof** Let $H$ and $H'$ be subgroups of $G$ belonging to the same orbit of $\mathfrak{P}(G)$. Then there exists $A \in \mathfrak{P}(G)$ such that $H \sim_G A$ and $H' \sim_G A$. Therefore, since $\sim_G$ is an equivalence relation on $\mathfrak{P}(G)$, it follows that $H \sim_G H'$ and so there exists $g \in G$ such that $H' = gH$. If $g \notin H$ then $g^{-1} \notin H^{-1}$, so that $e = gg^{-1} \notin gH = H'$. This contradicts the fact that $H'$ is a subgroup of $G$. Therefore $g \in H$ and so $H' = gH = H$.)

**c).** Let $p$ be a prime with $n = p^\alpha q$ and $\gcd(p, q) = 1$, where $\alpha := v_p(\mathrm{ord}(G))$. Let $\beta$ be a positive integer with $0 \leq \beta \leq \alpha$. Let $X \subseteq \mathfrak{P}_{p^\beta}(G)$ be a orbit of an element $A \in \mathfrak{P}_{p^\beta}(G)$ the above $G$-action. Then the following statments are equivalent:

(i) $v_p(\mathrm{card}(X)) \leq \alpha - \beta =: \gamma$. (ii) $\mathrm{card}(X) = p^{\alpha-\beta}$. (iii) $X$ contains exactly one subgroup $H$ (of order $p^\beta$). (**Proof** Let $A \in \mathfrak{P}_{p^\beta}(G)$ be such that the orbit of $A =: X$. By the orbit-stabiliser theorem 2)-d))

(c.1) $\mathrm{card}(G_A)\,\mathrm{card}(X) = \mathrm{card}(G) = p^\alpha q$ and so

(c.2) $\alpha = v_p(\mathrm{card}(G)) = v_p(\mathrm{card}(G_A)) + v_p(\mathrm{card}(X))$.

Since $G_A = \{g \in G \mid gA = A\}$, we have $ga \in A$ for every $g \in G_A$ and $a \in A$. Therefore, for any $a \in A$, there is a natural inclusion $G_A \cdot a \hookrightarrow A$. In particular, $\mathrm{card}(G_A) = \mathrm{card}(G_A \cdot a) \leq \mathrm{card}(A) = p^\beta$ and so $v_p(\mathrm{card}(G_A)) \leq \beta$. (i)$\Rightarrow$ (ii) : If $v_p(\mathrm{card}(X)) \leq \gamma$ then $v_p(\mathrm{card}(G_A)) = \beta$ by (c.2) above and so $\mathrm{card}(G_A) = p^\beta$. Therefore $\mathrm{card}(X) = p^\gamma q$ by (c.1) above. (ii)$\Rightarrow$ (iii): Since $\mathrm{card}(X) = p^\gamma q$, we have $v_p(\mathrm{card}(X)) = \gamma$ and so $v_p(\mathrm{card}(G_A)) = \beta$ by (c.2) above. Therefore $\mathrm{card}(G_A \cdot a)) = \mathrm{card}(G_A) = p^\beta$ and so $G_A \cdot a = A$ for every $a \in A$. Now, by 2)-e) $G_{a^{-1}A} = a^{-1} \cdot G_A \cdot a = a^{-1}A \in$ the orbit of $A = X$. Therefore $X$ contains a subgroup namely, $G_{a^{-1}A}$ and by the part b) this subgroup is unique. (iii)$\Rightarrow$ (i): Let $H$ be a subgroup of $G$ such that $H \in X$. Then $X$ is the orbit of $H = G/H = \{gH \mid g \in G\}$. Therefore $\mathrm{card}(X) = [G : H] = p^\alpha q / p^\beta = p^\gamma q$ and so $v_p(\mathrm{card}(X)) = \gamma$.)

**d).** With the notation as in the part c) above, there exists a natural number $t$ such that

$$\binom{p^\alpha q}{p^\beta} = \mathrm{d}_G(p, \beta) p^\gamma q + t p^{\gamma+1},$$

where $\mathrm{d}_G(p, \beta)$ is the number of subgroups of order $p^\beta$ and $\gamma = \alpha - \beta$. (**Proof** The action of $G$ on $\mathfrak{P}_{p^\beta}(G)$ gives a decomposition $\mathfrak{P}_{p^\beta}(G) = \bigcup\{\text{orbits with cardinality } = p^\gamma q\} \cup \bigcup\{\text{orbits with cardinality } \neq p^\gamma q\}$. Since the orbits with cardinality $= p^\gamma q$ are precisely the orbits which contains exactly one subgroup of $G$ of order $p^\beta$ (by the equivalence (i) $\iff$ (ii) of (c)) and the orbits with cardinality $\neq p^\gamma q$ are precisely the orbits whose cardinality is divisible by $p^{\gamma+1}$ (by the equivalence (i) $\iff$ (iii) of (c)), there exists a natural number $t$ such that $\binom{p^\alpha q}{p^\beta} = \mathrm{card}(\mathfrak{P}_{p^\beta}(G)) = d p^\gamma q + t p^{\gamma+1}$.)

**e).** In particular, if $G$ is cyclic in the part d) above then there exists a natural number $s$ such that $\binom{p^\alpha q}{p^\beta} = p^\gamma q + s p^{\gamma+1}$, where $\gamma := \alpha - \beta$. (**Proof** Since $\mathrm{card}(\mathfrak{P}_{p^\beta}(G))$ does not depend the group, the assertion follows from d) by taking $G$ to be the cyclic group.)

**24).** (Sylow theorems[5]) Let $G$ be a finite group of order $n$ and let $p$ be a prime divisor of $n$ with $n = p^\alpha q$ and $\gcd(p, q) = 1$, where $\alpha = v_p(\mathrm{Ord}\, G)$. Let $\beta$ be a non-negative integer with $0 \leq \beta \leq \alpha$ and let $\mathrm{d}_G(p, \beta)$ be the number f subgroups of $G$ of order $p^\beta$. Then

**a).** $\mathrm{d}_G(p, \beta) \equiv 1 (\mathrm{mod}\, p)$. In particular, $G$ has a subgroup of order $p^\alpha$. (**Proof** It follows from 23)-d) and e) that there exist natural numbers $s$ and $t$ such that $p^\gamma q + s p^{\gamma+1} = \binom{p^\alpha q}{p^\beta} = \mathrm{d}_G(p, \beta) p^\gamma q + t p^{\gamma+1}$, where $\gamma := \alpha - \beta$. Therefore $\mathrm{d}_G(p, \beta) q = q + (s - t)p \equiv q (\mathrm{mod}\, p)$ and so $\mathrm{d}_G(p, \beta) \equiv (\mathrm{mod}\, p)$, since $\gcd(p, q) = 1$. )

**b).** If $H$ is a subgroup of order $p^\alpha$ and $H'$ is a subgroup of order $p^\beta$, then there exist an element $g \in G$ such that $H' \subseteq gHg^{-1}$. In particular, any two subgroups of order $p^\alpha$ are conjugates in $G$. (**Proof**

[5]) These theorems were first proved by the Norwegian mathematician LUDWIG SYLOW (1832-1918) in 1872 [Sylow, L., Theoremes sur groups de substitutions, *Math. Ann.* **V**(1872), p. 584.]. We have given the proofs using elegant arguments due to WIELANDT, H., which is a great improvement over the older method of double cosets, see [Wielandt, H., Ein Beweis für die Exitenz der Sylowgruppes, *Archiv der Mathematik*, **vol. 10**(1959), p. 402-403.].

Restrict the operation (see 9)) of $G$ on the set of left-cosets $G/H$ of $H$ in $G$ to the subgroup $H'$. The class equation for this action is (see 3)-c)) $q = |G/H| \equiv |\mathrm{Fix}_{H'}(G/H)| \bmod p)$ and hence $\mathrm{Fix}_{H'}(G/H) \neq 0$, i.e. there exists a left-coset $gH$, $g \in G$ of $H$ in $G$ which is invariant under all left-translations of the elements from $H'$, i.e. $H' \subseteq gHg^{-1}$. restriction of the left-coset

**c).** $\mathrm{d}_G(p, \alpha)$ divides $q$ and so it divides $n$. (**Proof** By a) there is a subgroup $H$ of $G$ of order $p^\alpha$ and by b) all subgroups of order $p^\alpha$ are conjuagtes in $G$. But by 11)-d) the number of conjugate subgroups of $H$ in $G$ is the index $[G : \mathrm{N}_G(H)]$ of the normaliser $\mathrm{N}_G(H)$ of $H$ in $G$ and $[G : \mathrm{N}_G(H)]$ divides $[G : H] = q$.

**T8.3.** (Cycle polynomial and Polya's counting formula) Let $I$ be a finite set with cardinality $n \in \mathbb{N}^+$. For $\sigma \in \mathfrak{S}_n$, we put $Z^{\nu(\sigma)} := Z_1^{\nu_1} \cdots Z_n^{\nu_n}$, where $\nu(\sigma) = (\nu_1, \ldots, \nu_n)$ is the cycle type (see T8.1-5)) of $\sigma$. The Cycle-polynomial of a subgroup $H$ of the symmetric group $\mathfrak{S}_n$ is the polynomial $\Psi(H) := \dfrac{1}{\mathrm{card}(H)} \displaystyle\sum_{\sigma \in H} Z^{\nu(\sigma)}$ in indeterminates $Z_1, \ldots, Z_n$ (with coefficients in $\mathbb{Q}$).

For example:

**1). a).** The cycle-polynomial of the symmetric group $\mathfrak{S}_n$ is

$$\Psi(\mathfrak{S}_n) = \sum_{1\nu_1+2\nu_2+\cdots+n\nu_n} \frac{1}{\nu_1! \cdots \nu_n!} \left(\frac{Z_1}{1}\right)^{\nu_1} \cdots \left(\frac{Z_n}{n}\right)^{\nu_n}. \quad (\textbf{Hint:}\ \text{Use the Exercise 8.3-a).})$$

**b).** The cycle-polynomial of the alternating group $\mathfrak{A}_n$ is

$$\Psi(\mathfrak{A}_n) = 2 \cdot \sum_{\substack{1\nu_1+2\nu_2+\cdots+n\nu_n \\ \nu_2+\nu_4+\cdots+\nu_{2[n/2]} \equiv 0 \pmod 2}} \frac{1}{\nu_1! \cdots \nu_n!} \left(\frac{Z_1}{1}\right)^{\nu_1} \cdots \left(\frac{Z_n}{n}\right)^{\nu_n}$$

(**Hint:** Use the Exercise 8.3-a) and if $H$ is a subgroup of a finite group $G$ of index 2 then for every $x \in H$ either all conjugates of $x$ are in $H$ or exactly half of them are in $H$.)

**c).** The cycle-polynomail of the cyclic subgroup $\mathrm{Z}_n := \mathrm{H}(\langle 1, 2, \cdots, n\rangle)$ of $\mathfrak{S}_n$ genarted by the $n$-cycle $\langle 1, 2, \cdots, n\rangle$ is $\Psi(\mathrm{Z}_n) = \dfrac{1}{n} \displaystyle\sum_{d|n} \varphi(d) Z_d^{n/d}$, where $\varphi$ is the Euler's totient function.

**2).** Let $G$ be a finite group acting on a finite set $X$ of cardinality $n$ with the action homomorphism $\vartheta : G \to \mathfrak{S}(X)$. For $g \in G$, put $\nu(g) := \nu(\vartheta_g)$ and is called the cycle-type of $g \in G$. The polynomial $\Psi(G; \vartheta) = \Psi(G) := \dfrac{1}{\mathrm{card}(G)} \displaystyle\sum_{g \in G} Z^{\nu(g)}$ in indeterminates $Z_1, \ldots, Z_n$ over $\mathbb{Q}$ is called the cycle-polynomial of $G$ with respect to the action homomorphism $\vartheta$. Show that

**a).** $\Psi(G) = \Psi(H)$, where $H = \vartheta(G) \subseteq \mathfrak{S}(X)$.

**b).** Let $G$ be a finite group of order $n$. Show that the cycle polynomial of $G$ with respect to the Cayley's representation $\lambda : G \to \mathfrak{S}(G)$ of $G$ is $\Psi(G) = \dfrac{1}{n} \displaystyle\sum_{d|n} \alpha(d) Z_d^{n/d}$, where $\alpha(d) :=$ the number of elements of order $d$ in $G$. (**Hint:** Use the Exercise 8.5-a).)

**c).** Let $G$ and $H$ be finite groups acting on finite disjoint sets $X$ and $Y$, respectively. Then the product group $G \times H$ acts in a natural way on the disjoint union $X \cup Y$ as $(g, h) \cdot x := g \cdot x$ and $(g, h) \cdot y := h \cdot y$ for $g \in G, h \in H, x \in X, y \in Y$. Show that $\Psi(G \times H) = \Psi(G) \cdot \Psi(H)$.

**3).** Let $G$ be a finite group acting on a finite set $X$ with the action homomorphism $\vartheta : G \to \mathfrak{S}(X)$. Let $Y$ be any set (of colours) and let $\mathrm{C} := Y^X$ be the set of colourings of $X$ by the colours in $Y$. Then $G$ acts on the set C by: For $g \in G$ and $f \in \mathrm{C}$, $(g \cdot f)(x) := f(g^{-1}x)$ for $x \in X$. The basic problem is to find the cardinality of the quotient set $\overline{\mathrm{C}} := \mathrm{C}/G$ of patterns of colourings of $X$ with respect to the group $G$. A function $\gamma : Y \to A$ of $Y$ with values in any commutative ring $A$ with $\mathrm{ord}(G) \in A^\times =$ (the unit group of $A$) is called a weight function on $Y$ with values in $A$. For a weight function $\gamma : Y \to A$ and $f \in \mathrm{C}$, we put $\gamma(f) := \prod_{x \in X} \gamma(f(x))$. Then $\gamma$ induces a weight function $\overline{\gamma} : \overline{\mathrm{C}} \to A$ on the quotient set $\overline{\mathrm{C}}$.

**a).** (Pólya's counting formula [6]) Let $\pi_i := \sum_{y\in Y} \gamma(y)^i$, $i = 1, \ldots, n$, be the power-sums of the weights $\gamma(y)$, $y \in Y$. Then $\sum_{[f]\in\overline{\mathrm{C}}} \overline{\gamma}([f]) = \Psi(G)(\pi_1, \ldots, \pi_n)$. In particular, if $\mathrm{card}(Y) = m$ and if $\sigma_1, \ldots, \sigma_s \in$ is a representative system for the (distinct) conjugacy-classes of $G$, then $\mathrm{card}(\overline{\mathrm{C}}) = \Psi(G)(m, \ldots, m) = \frac{1}{|G|}\sum_{\sigma\in G} m^{|\nu(\sigma)|} = \sum_{i=1}^{s} \frac{m^{|\nu(\sigma_i)|}}{|\mathrm{Z}_G(\sigma_i)|}$. (**Proof:** Let $f \in \mathrm{C}$ and let $\sigma \in G$. Then $\sigma f = f$ if and only if $f$ is constant on the orbits $X_1, \ldots, X_s$ of $\sigma$, say $y_1, \ldots, y_s \in Y$. Therefore we have $\sum_{f\in \mathrm{Fix}_\sigma(\mathrm{C})} \gamma(f) = \sum_{(y_1,\ldots,y_s)\in Y^s} \gamma(y_1)^{\mathrm{card}(X_1)} \cdots \gamma(y_s)^{\mathrm{card}(X_s)} = \pi_{\mathrm{card}(X_1)} \cdots \pi_{\mathrm{card}(X_s)} = \pi_1^{\nu_1} \cdots \pi_n^{\nu_n} =: \pi^{\nu(\sigma)}$, where $\nu(\sigma) = (\nu_1, \ldots, \nu_n)$ is the cycle-type of $\sigma$. Now let $G_f$ denote the isotropy group at the point $f \in \mathrm{C}$. Then $\mathrm{ord}(G) \cdot \sum_{[f]\in\overline{\mathrm{C}}} \overline{\gamma}([f]) = \sum_{f\in\mathrm{C}} \mathrm{ord}(G_f) \cdot \gamma(f) = \sum_{(g,f),\, g\in G_f} \gamma(f) = \sum_{(g,f),\, f\in \mathrm{Fix}_\sigma(\mathrm{C})} \gamma(f) = \sum_{\sigma\in G} \pi^{\nu(\sigma)} = \mathrm{ord}(G) \cdot \Psi(G)(\pi_1, \ldots, \pi_n)$.)

**b).** Let $Y = \{y_i \mid i \in I\}$, $A = \mathbb{Q}[T_i \mid i \in I]$ be the polynomial ring in indeterminates $T_i$, $i \in I$ over $\mathbb{Q}$ and let $\gamma : Y \to A$ be the (monomial) weight function $y_i \mapsto \gamma(y_i) := T_i$. Then: *the coefficient of the monomial* $\prod_{i\in I} T_i^{\alpha_i}$, $(\alpha_i)_{i\in I} \in \mathbb{N}^{(I)}$, *in the polynomial* $\sum_{[f]\in\overline{\mathrm{C}}} \gamma([f]) = \Psi(G)(\pi_1, \ldots, \pi_n)$ *is the number of patterns* $[f] \in \overline{\mathrm{C}}$ *such that* $\alpha_i := |\{x \in X \mid f(x) = y_i\}|$ *for each* $i \in I$. (**Proof:** First note that for two colourings $f\, g \in \mathrm{C}$, if there exists a $\sigma \in G$ such that $\sigma f = g$, i.e., $[g] = [f]$ in the set of patterns $\overline{\mathrm{C}}$ (with respect to $G$), then $|f^{-1}(y_i)| = |g^{-1}(y_i)|$ for all $i \in I$. Further, if $f \in \mathrm{C}$ with $|f^{-1}(y_i)| = \alpha_i$ for all $i \in I$, then the weight of the pattern $[f]$ is $\gamma([f]) = \gamma(f) = \prod_{x\in X} \gamma(f(x)) = \prod_{i\in I} \gamma(y_i)^{\alpha_i} = \prod_{i\in I} T_i^{\alpha_i}$. Therefore $\sum_{[f]\in\mathrm{C},\ |f^{-1}(y_i)|=\alpha_i,\, i\in I} \gamma([f]) = \sum_{[f]\in\mathrm{C},\ |f^{-1}(y_i)|=\alpha_i,\, i\in I} \prod_{i\in I} T_i^{\alpha_i}$ and hence the proof.)

**4). a).** Deduce Fermat's little theorem from Pólya's counting formula.

**b).** On a stick of length $n$ feet the individual feet are marked consecutively $1, 2, \ldots, n$. The only symmetries are roratations about the center through the angles $0$ and $\pi$. Find the cycle-polynomial of this group of symmetries. Further, if each 1-foot segment can be painted one of $m$ colours. (1) How many patterns are possible? (2) if $n = 8$ and $m = 3$ ($Y := \{y_1, y_2, y_3\}$), in how many patterns are 2 segments $y_1$, 4 segments $y_2$ and 2 segments $G$ ?

**T8.4.** (Simplicial Complexes and Graphs) A simplicial complex $\mathcal{K}$ is a set $\mathbf{V}(\mathcal{K})$ called the vertex set (of $\mathcal{K}$) and a family of subsets of $\mathbf{V}(\mathcal{K})$, called simplexes (in $\mathcal{K}$) such that
(i) for each $v \in \mathbf{V}(\mathcal{K})$, the singleton set $\{v\}$ is a simplex in $K$.
(ii) if **s** is a simplex in $\mathcal{K}$ then so is every subset of **s**.

A simplex **s** in $\mathcal{K}$ is called a $q$-simplex if $\mathrm{card}(\mathbf{s}) = q + 1$ and say that **s** has dimension $q$. For a simplicial complex $\mathcal{K}$, we write $\dim(\mathcal{K}) := \sup\{q \mid \text{there exists a } q-\text{simplex in } \mathcal{K}\}$ and is called the dimension of $\mathcal{K}$. A simplicial complex of dimension $\leq 1$ is called a graph.

An edge in $\mathcal{K}$ is an ordered pair $(v_0, v_1)$ of vertices such that $\{v_0, v_1\}$ is a simplex in $\mathcal{K}$. If $\mathbf{e} = (v_0, v_1)$ is an edge in $\mathcal{K}$ the vertex $v_0$ (respectively $v_1$) is called the origin (respectively end) of **e** and usually denoted by $\mathrm{orig}(\mathbf{e})$ (respectively $\mathrm{end}(\mathbf{e})$).

A path $\alpha$ in $\mathcal{K}$ of length $n$ is a sequence $\mathbf{e}_1\mathbf{e}_2 \cdots \mathbf{e}_n$ of edges in $K$ with $\mathrm{end}(\mathbf{e}_i) = \mathrm{orig}(\mathbf{e}_{i+1})$ for every $1 \leq i \leq n-1$. For a path $\alpha = \mathbf{e}_1\mathbf{e}_2 \cdots \mathbf{e}_n$ we put $\mathrm{orig}(\alpha) = \mathrm{orig}(\mathbf{e}_1)$ and $\mathrm{end}(\alpha) := \mathrm{end}(\mathbf{e}_n)$ and say that $\alpha$ is a path from $\mathrm{orig}(\alpha)$ to $\mathrm{end}(\alpha)$.

A simplicial complex $\mathcal{K}$ is called connected if for every pair $(v_0, v_1)$ of vertices in $\mathcal{K}$ there exists a path $\alpha$ in $\mathcal{K}$ such that $\mathrm{orig}(\alpha) = v_0$ and $\mathrm{end}(\alpha) = v_1$.

---

[6]) See [G. Pólya: Kombinatorische Anzahlbestimmungen für Gruppen, Garphen und chemische Verbindungen, *Acta Mathematica,* **68,** 145-254, (1937).]