MA-219 Linear Algebra

11. Operations of Groups

11.1. A group G is called *homogeneous* if the natural action (see N11.6-a)) 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.

11.2. 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 T11.6.). Give an example to show that the assumption finite index is necessary. (**Hint:** $H = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in G \mid ac \neq 0 \right\} \neq G = \mathrm{GL}(2, \mathbb{C}) = \bigcup_{g \in G} gHg^{-1}$.)

11.3. Let G be a group and let X be a G-set. Show that

a). (*Burnside 's Formula*) $\mathrm{card}(G) \cdot \mathrm{card}(X/G) = \sum_{g \in G} \mathrm{card}(\mathrm{Fix}_g(X))$ (**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 $n(g) = \mathrm{card}(\mathrm{Fix}_g(X))$. Show that

(1) If G acts transitively on X then $\mathrm{card}(G) = \sum_{g \in G} n(g)$. Deduce that, if $\mathrm{card}(X) \geq 2$ and G acts transitively on X then there exists $g \in G$ such that $\mathrm{Fix}_g(G) = \emptyset$. (**Hint:** Use the Burnside 's formula.)
(2) If G acts 2-transitively on X then $2 \cdot \mathrm{card}(G) = \sum_{g \in G} n(g)^2$. (**Hint:** Use 11.7-c) and the part (1) above.)

11.4. (*Split-sequences*) Let $1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$ be an exact sequence of (not necessarily abelian) groups, i.e. φ is injective with $\mathrm{im}\,\varphi = \ker\psi$ and ψ is surjective (then $H \cong G/\mathrm{im}\,\varphi$ and $N \cong \mathrm{im}\,\varphi$.).

a). The group homomorphism ψ has a section, i.e. there exists a group homomorphismus $\sigma : H \to G$ such that $\psi\sigma = \mathrm{id}_H$ and so G is a semi-direct product of $\mathrm{im}\,\varphi \cong N$ and $\mathrm{im}\,\sigma \cong H$. In this case, we say that the short exact sequence $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is a *weak-split sequence* and the image $\mathrm{im}\,\sigma$ is called the *weak-complement* of $\mathrm{im}\,\varphi$ in G.

b). Suppose that there exists a projection $\pi : G \to N$ such that $\pi\varphi = \mathrm{id}_N$ and so G is a direct product of $\mathrm{im}\,\varphi \cong N$ and $\ker\pi \cong H$, i.e. the map $(x, y) \mapsto xy$ is a group isomorphism $\mathrm{im}\,\varphi \times \ker\pi \longrightarrow G$. In this case we say that the short exact sequence $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is a *(strong)-split sequence* and the kernel $\ker\pi$ is called a *strong-complement* of $\mathrm{im}\,\varphi$ in G.

c). Every (strong) split sequence is weak-split sequence. If σ is a section of ψ *and* $\mathrm{im}\,\sigma$ *is normal in* G, then $\mathrm{im}\,\sigma$ is a strong-complement of $\mathrm{im}\,\varphi$ and the sequence $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is (strong)-split.

d). If G (and hence H and N) is abelian, then $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is split sequence if and only if this sequence is weak-split.

e). If H is abelian, then the sequence $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is a split sequence if and only if the sequence $1 \longrightarrow N \cap \varphi^{-1}(\mathrm{Z}(G)) \longrightarrow \mathrm{Z}(G) \longrightarrow H \longrightarrow 1$ of abelian groups is exact and split, where $\mathrm{Z}(G)$ denote the center of G .) Every complement of $(\mathrm{im}\,\varphi) \cap \mathrm{Z}(G)$ in $\mathrm{Z}(G)$ is then a strong-complement of $\mathrm{im}\,\varphi$ in G.

11.5. Let N be a group. Then every semi-direct product (see N11.11) 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.)

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

a). $\mathrm{Fix}_G\, H$ 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 λ_n by n on H is bijektive. Then λ_n and the inverse $(\lambda_n)^{-1}$ of λ_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 $\mathrm{Fix}_G H$, i.e. $\pi_H = \pi_H^2$ and $\mathrm{im}\,\pi_H = \mathrm{Fix}_G H$. (**Hint:** Let $\pi := \pi_H$. The inclusion $\pi(H) \subseteq \mathrm{Fix}_G H$ is mentioned in the part b). Conversely, let $x \in \mathrm{Fix}_G H$, then $\pi x = \frac{1}{n}\sum_{g\in G} gx = \frac{1}{n} nx = x$. This proves the inclusion $\mathrm{Fix}_G H \subseteq \pi(H)$ 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 [1]), then the induced sequence $\mathrm{Fix}_G H' \to \mathrm{Fix}_G H \to \mathrm{Fix}_G H''$ is also exact. (**Hint:** For $x \in \mathrm{Fix}_G H$ with $f(x) = 0$ we need to find $x' \in \mathrm{Fix}_G H'$ with $f'(x') = x$. Let $\widetilde{x} \in H'$ be such that $f'(\widetilde{x}) = x$. Then $x' := \pi'_H(\widetilde{x}) \in \mathrm{Fix}_G H'$ 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 N11.6-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.)

On the other side one can see (simple) test-exercises; their solutions need not be submitted.

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

Operations of groups

Below we collect definitions, basic results and examples on operations of groups.

N11.1. (Group actions --action homomorphisms and G-sets) 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 $\vartheta_e = \mathrm{id}_X$ and $\vartheta_{gh} = \vartheta_g \vartheta_h$ by the conditions (1) and (2) above, respectively. In particular, for every $g \in G$, the map ϑ_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.

N11.2. (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 $x \in X$, $G_x := \{g \in G \mid gx = x\}$ 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) $\mathrm{card}(Gx) = [G : G_x]$, 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 $\mathrm{card}(Gx)$ divides the order of the group G.

e). For $g \in G, x \in X$, $G_{gx} = gG_xg^{-1}$. 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 $\mathrm{Fix}_g(X)$. If $E \subseteq G$ then we put $\mathrm{Fix}_E(X) := \cap_{g\in E} \mathrm{Fix}_g(X)$. The elements of $\mathrm{Fix}_G(X)$ are called fixed elements of the operation of G on X. An element $x \in X$ belongs to $\mathrm{Fix}_G(X)$ if and only if $G_x = G$.

N11.3. 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 ϑ 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 $\operatorname{card}(G)$ 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 ϑ 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 $\operatorname{card}(X) = [G : G_x]$. In particular, if G is finite then X is finite and $\operatorname{card}(X)$ divides $\operatorname{card}(G)$.

N11.4. (Class Equation) Let G be a group operating on a set X. Then

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

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 cation 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 $\operatorname{card}(G) = \operatorname{card}(H) \cdot \operatorname{card}(G/H)$. 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,* $\operatorname{ord}(G) = \operatorname{ord}(H) \cdot [G : H]$.

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 $\kappa : G \to \operatorname{Aut}(G)$, $g \mapsto \kappa_g : G \to G$, $x \mapsto gxg^{-1}$. The fixed point set of this operation is the center $\mathrm{Z}(G)$ 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:

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

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

c). 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 $\operatorname{card}(X) \equiv \operatorname{card}(\operatorname{Fix}_G(X)) \pmod{p}$. In particular, the center $\mathrm{Z}(G)$ of G is non-trivial. (**Hint:** For the last part use the class equation for G.)

d). (Cauchy's theorem and Fermat's little theorem) 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 c) $\operatorname{card}(X) = n^{p-1} \equiv |\operatorname{Fix}_H X| \bmod p$.

(1) If p divides n, then p also divides $|\operatorname{Fix}_H X|$, 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 $\operatorname{Fix}_H X$ 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. $n^{p-1} \equiv 1 \bmod p$.*

N11.5. 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 N11.3-c)) of G on $X = Y = G$.)

N11.6. (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 $\operatorname{im}(\vartheta) \subseteq \operatorname{Aut}(H) =$ (the set of all automorphisms of the group H) then we say that G acts on H by automorphisms or ϑ is an automorphism action and in this case we write $\vartheta : G \to \operatorname{Aut}(H)$ instead of $\vartheta : G \to \mathfrak{S}(H)$.

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

b). The conjugate action of the group G on G is the automorphism action $\kappa : G \to \operatorname{Aut}(G)$, $g \mapsto \kappa_g$, 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.

N11.7. (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 $(x_1, \dots, x_k) \in X^k$ with $x_i \neq x_j$ for $1 \le i \neq j \le k$ and $(y_1, \dots, y_k) \in X^k$ with $y_i \neq y_j$ for $1 \le i \neq j \le k$, there exists an element $g \in G$ such that $\vartheta(g)(x_i) = y_i$ for every $1 \le i \le k$. 1-transitive is same as transitive (see N11.3 -(1)).

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

b). For $n \in \mathbb{N}^+$, any subgroup of $\mathfrak{S}_n$ acts naturally on the set $\{1, \dots, n\}$, 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 $\{1, \dots, n\}$ is n-transtive (respectively, $(n-2)$-transitive but not $(n-1)$-transitive).

c). The subset $X^{(n)} := \{(x_1, \dots, x_n) \mid x_i \in X, x_i \neq x_j, 1 \le i \neq j \le n\}$, $(n \in \mathbb{N}^+)$ of X^n is a G-subset of the diagonal action (see N11.5-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 $\operatorname{ord}(G)$. (**Hint:** Use N11.3-g).)

N11.8. (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 ϑ. 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 $N = \bigcap_{g\in G} gHg^{-1}$ 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 $F \subseteq \bigcap_{g\in G} gHg^{-1} = N$)

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.)

N11.9. (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

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

of groups and group homomorphisms is commutative, where ϑ_X, ϑ_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). Moregenerally, 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 *φ-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 $f : X \to Y$ φ-invariant if and only if f is a G-invariant map, where the H-operation on Y via φ defines a G-operation on Y, i.e. $gy := \varphi(g)y$, $g \in G$, $y \in Y$.

N11.10. (*Semi-direct Product – Holomorph of a group*) Let N and H be groups. Suppose that H operates on N by automorphisms (see N11.6), 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 ϑ 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 ϑ 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 ϑ 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 λ_n for $n \in N$ denote the left-translation by n.

d). The subgroup 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 Hol (N) also contain right-translationen.

N11.11. (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 N11.6), 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. [2])

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 $\mathbf{D}_\infty$.

N11.12. 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 $A \mapsto gA := \{ga \mid a \in A\}$.

a). For every fixed positive integer $r \le n$, the subset $\mathfrak{P}_r(G) := \{A \in \mathfrak{P}(G) \mid \operatorname{card}(A) = r\}$ 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 $\alpha := v_p(\operatorname{ord}(G))$. Let β be a positive integer with $0 \le \beta \le \alpha$. 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) $v_p(\operatorname{card}(X)) \le \alpha - \beta =: \gamma$. (ii) $\operatorname{card}(X) = p^{\alpha-\beta}$. (iii) X contains exactly one subgroup H (of order p^β). (**Proof** Let $A \in \mathfrak{P}_{p^\beta}(G)$ be such that the orbit of $A =: X$. By the orbit-stabiliser theorem (N11.2-d))

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

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

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, $\operatorname{card}(G_A) = \operatorname{card}(G_A \cdot a) \le \operatorname{card}(A) = p^\beta$ and so $v_p(\operatorname{card}(G_A)) \le \beta$. (i)$\Rightarrow$(ii) : If $v_p(\operatorname{card}(X)) \le \gamma$ then $v_p(\operatorname{card}(G_A)) = \beta$ by (c.2) above and so $\operatorname{card}(G_A) = p^\beta$. Therefore $\operatorname{card}(X) = p^\gamma q$ by (c.1) above. (ii)$\Rightarrow$(iii): Since $\operatorname{card}(X) = p^\gamma q$, we have $v_p(\operatorname{card}(X)) = \gamma$ and so $v_p(\operatorname{card}(G_A)) = \beta$ by (c.2) above. Therefore $\operatorname{card}(G_A \cdot a)) = \operatorname{card}(G_A) = p^\beta$ and so $G_A \cdot a = A$ for every $a \in A$. Now, by N11.2-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 $\operatorname{card}(X) = [G : H] = p^\alpha q / p^\beta = p^\gamma q$ and so $v_p(\operatorname{card}(X)) = \gamma$.)

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

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

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

---

[2]) 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.

e). In particular, if G is cyclic in the part d) above then there exists a natural number s such that $\binom{p^\alpha q}{p^\beta} = p^\gamma q + sp^{\gamma+1}$, where $\gamma := \alpha - \beta$. (**Proof** Since $\mathrm{card}(\mathfrak{P}_{p^\beta}(G))$ does not depend the group, the assertion follows from (5) by taking G to be the cyclic group.)

N11.13. (Sylow theorems[3])) 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 β be a non-negative integer with $0 \le \beta \le \alpha$ and let $\mathrm{d}_G(p,\beta)$ be the number f subgroups of G of order p^β. Then

a). $\mathrm{d}_G(p,\beta) \equiv 1 (\mathrm{mod}\, p)$. In particular, G has a subgroup of order p^α. (**Proof** It follows from N11.12-d) and e) that there exist natural numbers s and t such that $p^\gamma q + sp^{\gamma+1} = \binom{p^\alpha q}{p^\beta} = \mathrm{d}_G(p,\beta)p^\gamma q + tp^{\gamma+1}$, 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^α and H' is a subgroup of order p^β, then there exist an element $g \in G$ such that $H' \subseteq gHg^{-1}$. In particular, any two subgroups of order p^α are conjugates in G. (**Proof** Restrict the operation (see N11.8) 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 N11.4-c)) $q = |G/H| \equiv |\mathrm{Fix}_{H'}(G/H)| \bmod p$) and hence $\mathrm{Fix}_{H'}(G/H) \ne 0$, 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^α and by b) all subgroups of order p^α are conjuagtes in G. But by T11.6-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 $[G : H] = q$.

Test-Exercises

T11.1. Let V be a n-dimensional vector space over a field K, $n \in \mathbb{N}^+$ and let $G := \mathrm{Aut}_K(V) = GL_K(V)$ 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.

a). 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 $v \in V \setminus \{0\}$.

b). 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 $(v_1, \ldots, v_n) \in \mathcal{B}$.

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

d). 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 $0 \le i \le n$. 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 $(V_0 \subset V_1 \subset \cdots \subset V_n) \in \mathcal{F}$.

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

T11.2. 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). 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 $\vartheta\psi$.

b). If $\varphi : G \to G''$ is a surjective group homomorphism such that the kernel $\mathrm{Ker}\,\varphi \subseteq \mathrm{Ker}\,\vartheta$, 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 $\vartheta : G \to \mathfrak{S}(X)$.

c). 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.

d). 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

[3]) 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.].

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 $\mathrm{Fix}_G(Y) = Y$.)

e). 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 λ_X^Y is defined in the footnote [4]) 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.

f). 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 ρ_X^Y is defined in the footnote [4]) and the fixed set $\mathrm{Fix}_G(Y^X) = \{f \in X^Y \mid f \text{ is constant on the } G\text{-orbits of } X\}$.

g). 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 μ_{YX} is defined in the footnote [4]). 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 $\mathrm{Fix}_G(Y^X) = \mathrm{Hom}_G(X,Y) = \{f \in Y^X \mid f \text{ is a } G\text{-homomorphism}\}$.

T11.3. 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 N11.8).)

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.

d). (Yang) If G is finite and H is a subgroup of prime index p, where p is the smallest prime divisor of $\mathrm{Ord}\,G$, 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 $\mathrm{ord}(G) = mn$, $\mathrm{ord}(H) = n$.

(1) Let N be the kernel of the action of the left coset G-set G/H. Then $[H:N]$ divides $\gcd(n, (m-1)!)$.
(2) (Frobenius) If n has no prime factor less than m then H is normal in G. (**Hint:** Use (1) above.)
(3) If $\mathrm{ord}(G) = 2^r \cdot 3$ 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 ϑ has the cardinality $= \mathrm{card}(H)$.

T11.4. Let p be a prime number. Then

---

[4]) **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.

a). 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 N11.4-c).)

b). Every group of order $2p$ is either cyclic or isomorphic to the Dihedral group D_p . (**Remark:** The case $p = 2$ is a special case. – For a generalisation see exercise set 12 on affine maps)

c). 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 N11.3-h). **Remark** There exists infinite groups of class number 2.)

T11.5. Let G be a finite group of odd order and let $x \in G,\ x \neq e$. Show that $\mathrm{C}_G(x) \neq \mathrm{C}_G(x^{-1})$, i.e. x and x^{-1} belongs to different conjugacy classes. (**Hint:** If $\mathrm{C}_G(x) = \mathrm{C}_G(x^{-1})$, then show that $\mathrm{card}(\mathrm{C}_G(x))$ is even. But by N11.4-b) $\mathrm{card}(\mathrm{C}_G(x))$ divides the order $\mathrm{ord}(G)$ of G a contradiction.)

T11.6. 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 n o r m a l i s e r of A in G and is denoted by $\mathrm{N}_G(A)$.

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

b). The kernel of this operation of $\mathrm{N}_G(A)$ on A is the c e n t r a l i s e r $\mathrm{C}_G(A) = \bigcap_{a\in A}\mathrm{C}_G(a)$ of A. In particular, $\mathrm{C}_G(A)$ is normal in $\mathrm{N}_G(A)$.

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

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

T11.7. 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 (N11.4-d)(1)). –**Remark:** A group in which order of every element G is a power of a prime number p, is called a p- g r o u p .)

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 (N11.4-d)(1)).)

T11.8. Let X be a G-set. A subset Y of X is called a G - s u b s e t 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 N11.8) 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.)

T11.9. 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.)