Groups (including additional problems)

1. Groups

**Definition 1.1 (Group).** A group is a set $G$ together with a binary operation $*$ on $G$ such that the following properties hold:

(G1) For all $a, b, c \in G$ we have

$$a \ast (b \ast c) = (a \ast b) \ast c.$$  

(G2) There exists an element $e \in G$, called an identity element or a neutral element, such that for every $a \in G$ we have

$$a \ast e = e \ast a = a.$$  

(G3) For every $x \in G$ there exists an element $y \in G$, called an inverse of $x$ such that

$$x \ast y = y \ast x = e,$$

where $e \in G$ is an identity element.

**Remark 1.2.** Let $G$ be a set with a binary operation $*$.  

(1) Suppose $e_1, e_2 \in G$ both satisfy axiom (G2) above. Then $e_1 = e_2$.  

Thus if $(G, *)$ is a group then there exists a unique element $e \in G$ satisfying (G2). This element $e \in G$ is called the identity element or the neutral element in $G$ and sometimes is denoted $e_G$.  

(2) Suppose $G$ satisfies axioms (G1) and (G2) and let $x, y_1, y_2 \in G$ be such that

$$x \ast y_1 = y_1 \ast x = e, \quad \text{and} \quad x \ast y_2 = y_2 \ast x = e.$$  

Then $y_1 = y_2$.  

Thus if $(G, *)$ then for every $x \in G$ there exists a unique element $y \in G$ satisfying $x \ast y = y \ast x = e$. This element $y \in G$ is called the inverse of $x$ in $G$ and is sometimes denoted $y = x^{-1}$.  

**Convention 1.3.** If $(G, *)$ is a group and the group operation $*$ is written multiplicatively rather than additively, then for $a, b \in G$ we often denote

$$ab = a \ast b.$$  

**Definition 1.4 (Abelian group).** Let $(G, *)$ be a group. This group is called abelian or commutative if for all $a, b \in G$ we have $a \ast b = b \ast a$.  

**Example 1.5.**  

(1) $(\mathbb{R}, +)$ is an abelian group, where $+$ is the standard addition of real numbers.  

(2) For every $n \in \mathbb{N}$, $(\mathbb{R}^n, +)$ is an abelian group, where $+$ is the standard vector addition.  

(3) $(\mathbb{R}, \cdot)$ is not an abelian group (where $\cdot$ is the standard multiplication). The axioms (G1) and (G2) do hold, with $1 \in \mathbb{R}$ being the identity element with respect to $\cdot$. However, (G3) fails, since the element $0 \in \mathbb{R}$ does not admit a multiplicative inverse in $\mathbb{R}$.  

(4) $(\mathbb{R}^\times, \cdot)$ is an abelian group, where $\mathbb{R}^\times = \mathbb{R} - \{0\}$.  

(5) $(\mathbb{N}, +)$ is not a group: (G1) holds but (G2) fails.
(6) Let $\mathbb{Z}_{\geq 0} = \{ n \in \mathbb{Z} : n \geq 0 \}$. Then $(\mathbb{Z}_{\geq 0}, +)$ is not a group, since (G1) and (G2) hold but (G3) fails. For example, $1 \in \mathbb{Z}_{\geq 0}$ does not admit an additive inverse in $\mathbb{Z}_{\geq 0}$.

(7) For a nonempty set $X$ denote by $\text{Sym}(X)$ the set of all bijections $f : X \to X$. Then $(\text{Sym}(X), \circ)$ is always a group, where $\circ$ is the composition of functions. This group is called the symmetric group on $X$. If $|X| \geq 3$, the group $\text{Sym}(X)$ is nonabelian. If $|X| \leq 2$, the group $\text{Sym}(X)$ is abelian.

For $n \in \mathbb{N}$ and $X_n = \{1, 2, \ldots, n\}$, the group $\text{Sym}(X_n)$ is denoted $S_n$ and is called the symmetric group of rank $n$.

(8) Let $(F, +, \cdot)$ be a field. Denote $F^\times := \{ a \in F : a \neq 0 \}$. Then $(F^\times, \cdot)$ is an abelian group.

(9) Let $(F, +, \cdot)$ be a field. Then $(F, +)$ is an abelian group.

(10) For $n \in \mathbb{N}$ denote by $M_{n,n}(\mathbb{R})$ the set of all $n \times n$-matrices with entries in $\mathbb{R}$. Let $+$ and $\cdot$ be the standard matrix addition and multiplication.

Then $(M_{n,n}(\mathbb{R}), +)$ is an abelian group, but $(M_{n,n}(\mathbb{R}), \cdot)$ is not a group since axiom (G3) fails.

(11) For $n \in \mathbb{N}$ let $GL(n, \mathbb{R}) = \{ A \in M_{n,n}(\mathbb{R}) : \det(A) \neq 0 \}$. Then $GL(n, \mathbb{R})$, with the standard matrix multiplication, is a group. This group is abelian for $n = 1$ and nonabelian for $n \geq 2$.

(12) Let $m \geq 2$ be an integer. Let $+, \cdot$ be the standard addition and multiplication on the set $\mathbb{Z}_m$. Then $(\mathbb{Z}_m, +)$ is an abelian group.

Also, denote

$$\mathbb{Z}_m^n = \{ [n]_m \in \mathbb{Z}_m : \text{there is } x \in \mathbb{Z} \text{ such that } [n]_m[x]_m = [1]_m \}. $$

Then $(\mathbb{Z}_m^n, \cdot)$ is an abelian group.

(13) For $n \in \mathbb{N}$ and an integer $m \geq 2$ let $SL(n, m)$ be the set of all $n \times n$ matrices $A$ with entries from $\mathbb{Z}_m$ such that $\det(A) = [1]_m$ (here the determinant of $A$ is computed by the same procedure as for a matrix with entries from $\mathbb{Z}$). Then $SL(n, m)$, with the standard matrix multiplication, is a group.

**Notation 1.6.** Let $X$ be a set and let $a_1, \ldots, a_n \in X$ be $n$ distinct elements in $X$, where $n \in \mathbb{N}$. We denote by $(a_1, a_2 \ldots, a_n) \in \text{Sym}(X)$ the bijection $f : X \to X$ defined as follows: $f(a_1) = a_2$, $f(a_2) = a_3$, \ldots, $f(a_{n-1}) = a_n$, $f(a_n) = a_1$ and $f(x) = x$ for all $x \in X \setminus \{a_1, \ldots, a_n\}$. We call such an element of $\text{Sym}(X)$ an $n$-cycle.

**Proposition 1.7** (Basic properties of groups). Let $(G, \cdot)$ be a group. Then:

1. If $n \geq 2$ is an integer and $a_1, \ldots, a_n \in G$, then any two ways of placing the parentheses to specify the sequence of multiplications in the expression $a_1 \cdots a_n$ produce the same element of $G$. This element is denoted $a_1 \ldots a_n$.
2. For any $a, b \in G$ we have
   $$(ab)^{-1} = b^{-1}a^{-1}.$$  
3. For any $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in G$ we have
   $$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$ 
4. For every $a \in G$ we have $(a^{-1})^{-1} = a$.
5. If $a, x, y \in G$ are such that $ax = ay$ then $x = y$.
6. If $a, x, y \in G$ are such that $xa = ya$ then $x = y$. 
Proof. (1) This statement follows from associativity of multiplication and can be proved by strong induction on \( n \). We omit the details.

(2) Put \( y = b^{-1}a^{-1} \). We will check that \( y(ab) = (ab)y = e_G \). By the definition of inverses this will imply that \( y = (ab)^{-1} \).

Indeed

\[
y(ab) = b^{-1}a^{-1}ab = b^{-1}e_Gb = b^{-1}b = e_G
\]

and

\[
(ab)y = abb^{-1}a^{-1} = ae_Ga^{-1} = aa^{-1} = e_G.
\]

(3) This statement can be proved by induction on \( n \) in a similar way to part (2).

We leave part (4) as an exercise.

(5) Suppose that \( ax = ay \) in \( G \).

Then

\[
a^{-1}(ax) = a^{-1}(ay).
\]

By associativity, \( a^{-1}(ax) = (a^{-1}a)x = e_Gx = x \) and, similarly \( a^{-1}(ay) = (a^{-1}a)y = e_Gy = y \). Hence \( x = y \).

The proof of (6) is similar to (5).

\[\square\]

Definition 1.8. Let \( G \) be a group and let \( a, b \in G \). We say that \( a \) and \( b \) are conjugate in \( G \) if there exists \( h \in G \) such that \( b = hgh^{-1} \).

Definition 1.9 (Powers). Let \( (G, \cdot) \) be a group and let \( a \in G \).

(1) For \( n \in \mathbb{N} \) define \( a^n \in G \) inductively by setting \( a^1 := a \) and \( a^n := a^{n-1}a \) for \( n \geq 2 \).

(2) Put \( a^0 := e_G \).

(3) For \( n \in \mathbb{N} \) put \( a^{-n} := (a^n)^{-1} \).

Thus we have defined \( a^n \) for every \( a \in G \) and every \( n \in \mathbb{Z} \).

Proposition 1.10. Let \( (G, \cdot) \) be a group and let \( a \in G \). Then:

(1) For every \( n \in \mathbb{Z} \) we have \( a^{-n} = (a^n)^{-1} = (a^{-1})^n \).

(2) For all \( n, m \in \mathbb{Z} \) we have \( a^{n+m} = a^na^m \).

(3) For all \( n, m \in \mathbb{Z} \) we have \( (a^n)^m = a^{nm} \).

(4) For any \( g \in G \) and \( n \in \mathbb{Z} \) we have \( (gag^{-1})^n = ga^n g^{-1} \).

1.1. Additional problems.

(1) Is \( \mathbb{Z} \), with the standard multiplication of integers, a group?

(2) Is \( GL(2, \mathbb{R}) \) a group with respect to the matrix addition? [Hint: Check first whether matrix addition is a binary operation on \( GL(2, \mathbb{R}) \)].

(3) Is \( \mathbb{Z}_5 \), with the standard multiplication of congruence classes, a group?

(4) Is \( \mathbb{R}[x] \), with the standard addition of polynomials, a group?

(5) Is \( \mathbb{R}[x] \), with the standard multiplication of polynomials, a group?

(6) For \( n \in \mathbb{N} \) denote \( SL(n, \mathbb{R}) := \{ A \in GL(n, \mathbb{R}) : \det(A) = 1 \} \). Determine whether or not \( SL(n, \mathbb{R}) \), with the standard matrix multiplication, is a group.

(7) Let \( X \) be a nonempty set, and let \( (G, \ast) \) be a group. Let \( F(X, G) \) be the set of all functions \( f : X \rightarrow G \). Define a binary operation \( \cdot \) on \( F(X, G) \) as follows. For \( f, h : X \rightarrow G \) define \( f \cdot h : X \rightarrow G \) as \( (f \cdot h)(x) = f(x) \ast h(x) \), where \( x \in X \).

Prove that \( (F(X, G), \cdot) \) is a group. Then show that this group is abelian if and only if \( G \) is abelian.
(8) Compute $|SL(2, 2)|$.

(9) Show that if $X$ is a set, $(a_1 \ a_2 \ \ldots \ a_n) \in Sym(X)$ is an $n$-cycle and $f \in Sym(X)$ then

$$f(a_1 \ a_2 \ \ldots \ a_n)f^{-1} = (f(a_1) \ f(a_2) \ \ldots \ f(a_n))$$

in $Sym(X)$, so that a conjugate of an $n$-cycle is again an $n$-cycle.

2. SUBGROUPS

**Definition 2.1** (Subgroup). Let $(G, \ast)$ be a group. A subset $H \subseteq G$ is called a subgroup of $G$, denoted $H \leq G$, if the following hold:

(1) For any $x, y \in H$ we have $x \ast y \in H$.

(2) We have $e_G \in H$.

(3) For any $x \in H$ we have $x^{-1} \in H$ (where $x^{-1}$ is the inverse of $x$ in $G$).

The notion of a subgroup is particularly important in view of the following:

**Proposition 2.2.** Let $(G, \ast)$ be a group and let $H \leq G$ be a subgroup. For $a, b \in H$ define $a \ast_H b := a \ast b$.

Then $\ast_H$ is a binary operation on $H$ and $(H, \ast_H)$ is a group.

**Example 2.3.**

(1) We have $\mathbb{Z} \leq \mathbb{R}$ where $(\mathbb{R}, +)$ is a considered as a group with the standard addition.

(2) We have $\mathbb{N} \leq \mathbb{R}$ where $(\mathbb{R}, +)$ is a considered as a group with the standard addition.

(3) We have $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$ where $GL(n, \mathbb{R})$ is viewed as a group with the standard matrix multiplication.

(4) Let $X \neq \varnothing$ and $x \in X$. Put $Stab(x) := \{f \in Sym(X) : f(x) = x\}$. Then $Stab(x) \leq Sym(X)$.

(5) The set $H = \{[0]_4, [2]_4\}$ is a subgroup of $(\mathbb{Z}_4, +)$.

(6) For any $n \in \mathbb{N}$, the set $\mathbb{Z}^n$ is a subgroup of $(\mathbb{R}^n, +)$.

(7) Let $X \neq \varnothing$ and $(G, \ast)$ be a group. Let $x \in X$. Put $H = \{f \in \mathcal{F}(X, G) : f(x) = e_G\}$. Then $H \leq \mathcal{F}(X, G)$.

**Proposition 2.4.** Let $G$ be a group and let $H_1 \leq G$ and $H_2 \leq G$ be two subgroups. Then $H_1 \cap H_2 \leq G$.

**Proposition-Definition 2.5** (Conjugate subgroups). Let $G$ be a group and let $g \in G$. Then the set

$$H^g := \{ghg^{-1} : h \in H\}$$

is a subgroup of $G$.

We sometimes denote the $H^g$ by $gHg^{-1}$.

We say that subgroups $H_1, H_2 \leq G$ are conjugate in $G$ if there exists $g \in G$ such that $H_1^g = H_2$.

**Definition 2.6** (Normal subgroup). Let $G$ be a group and let $H \leq G$ be a subgroup of $G$. We say that $H$ is a normal subgroup of $G$, denoted $H \trianglelefteq G$, if for every $g \in G$ and every $h \in H$ we have $ghg^{-1} \in H$.

**Example 2.7.**

(1) If $G$ is a group and $a, g \in G$ then $\langle a \rangle^g = \langle gag^{-1} \rangle$ (see Definition 2.9 below for the definition of $\langle a \rangle$).
Proposition 2.9 (Cyclic subgroup). Let \( G \) be a group and let \( H \leq G \) be a subgroup. Then \( H \triangleleft G \) if and only if for every \( g \in G \) we have \( H^g = H \).

Proof. It is obvious that if for every \( g \in G \) we have \( H^g = H \) then \( H \triangleleft G \).

Suppose now that \( H \triangleleft G \) and let \( g \in G \) be arbitrary. Since \( H \triangleleft G \), for every \( h \in H \) we have \( ghg^{-1} \in H \) and hence \( H^g \subseteq H \). We claim that we also have \( H \subseteq H^g \).

Indeed, let \( h \in H \) be arbitrary. Put \( b = g^{-1} \). Since \( H \triangleleft G \), we have \( bb^{-1} = 1 \in H \), that is \( g^{-1}hg \in H \), that is, \( g^{-1}hg = h_1 \) for some \( h_1 \in H \). From \( g^{-1}hg = h_1 \) we get \( h = gh_1g^{-1} \), so that \( h \in H^g \). Since \( h \in H \) was arbitrary, this implies \( H \subseteq H^g \), as claimed. Since we already know that \( H^g \subseteq H \), it follows that \( H^g = H \), as required. \( \square \)

Proposition-Definition 2.9 (Cyclic subgroup). Let \( G \) be a group and let \( a \in G \). Put

\[
\langle a \rangle := \{a^n : n \in \mathbb{Z}\}.
\]

Then \( \langle a \rangle \leq G \).

The subgroup \( \langle a \rangle \) is called the **cyclic subgroup of \( G \) generated by \( a \)**.

Proof. Since for any \( m, n \in \mathbb{Z} \) we have \( a^m a^n = a^{m+n} \), property (1) of Definition 2.1 holds for \( \langle a \rangle \).

We also have \( a^0 = e_G \), so that \( e_G \in \langle a \rangle \) and thus property (2) of Definition 2.1 holds for \( \langle a \rangle \) also holds.

Finally, since for every \( n \in \mathbb{Z} \) we have \( (a^n)^{-1} = a^{-n} \), property (3) of Definition 2.1 holds for \( \langle a \rangle \) also holds. Thus Indeed \( \langle a \rangle \leq G \). \( \square \)

Definition 2.10 (Cyclic group). A group \( G \) is called **cyclic** if there exists \( a \in G \) such that \( \langle a \rangle = G \).

Definition 2.11 (Order of an element). Let \( G \) be a group and let \( a \in G \).

If there does not exist \( n \in \mathbb{N} \) such that \( a^n = e_G \), we put \( \text{ord}(a) = \infty \) and say that \( a \) has **infinite order** in \( G \).

Suppose that there exists \( n \in \mathbb{N} \) such that \( a^n = e_G \). Then we put

\[
\text{ord}(a) := \min\{n \in \mathbb{N} : a^n = e_G\}
\]

and call the number \( \text{ord}(a) \in \mathbb{N} \) the **order of \( a \)** in \( G \).

Theorem 2.12. Let \( G \) be a group and let \( a \in G \).

(1) If \( \text{ord}(a) = \infty \) then \( \langle a \rangle \) is countably infinite.

(2) If \( \text{ord}(a) = n \in \mathbb{N} \) then the group \( \langle a \rangle \) is finite and \( |\langle a \rangle| = n = \text{ord}(a) \).

2.1. Additional problems.

(1) Show that if \( G \) is a cyclic group then the set \( G \) is countable.

(2) Show that for the group \((\mathbb{Z}, +)\) we have \( \mathbb{Z} = \langle 1 \rangle \), so that \((\mathbb{Z}, +)\) is cyclic.

(3) Show that \((\mathbb{Q}, +)\) is not cyclic.

(4) Show that \((\mathbb{Z}^2, +)\) is not cyclic.

(5) Show that if \( m \geq 2 \) is an integer then for the group \((\mathbb{Z}_m, +)\) we have \( \mathbb{Z}_m = \langle [1]_m \rangle \), so that \((\mathbb{Z}_m, +)\) is cyclic.

(6) Show that every cyclic group is abelian.

(7) Show that the group \( S_3 \) is not cyclic.

(8) Show that the group \((\mathbb{Z}_5^\times, \cdot)\) is cyclic.
(9) Show that
\[
H = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}
\]
is a subgroup of \(GL(2, \mathbb{R})\).
(10) Show that if \(g = (a_1 \ a_2 \ldots \ a_n) \in \text{Sym}(X)\) then \(\text{ord}(g) = n\).
(11) Show that \(\langle 1 \ 2 \rangle \notin \text{Sym}_3\).
(12) Prove that if \(X\) is a set, \(x, y \in X\) and \(f \in \text{Sym}(X)\) is such that \(f(x) = y\) then \(f\text{Stab}(x)f^{-1} = \text{Stab}(y)\) in \(\text{Sym}(X)\).
(13) Show that if \(X\) is a set with \(|X| \geq 3\) and \(x \in X\) then \(\text{Stab}(x) \notin \text{Sym}(X)\).
(14) Denote
\[
\text{SL}(n, \mathbb{Z}) := \{ A \in \text{SL}(n, \mathbb{R}) \mid \text{all entries of } A \text{ belong to } \mathbb{Z} \}.
\]
Prove that \(\text{SL}(n, \mathbb{Z}) \leq \text{SL}(n, \mathbb{R})\).
(15) Show that \(\text{SL}(2, \mathbb{Z}) \not\sub \text{SL}(2, \mathbb{R})\).

3. Cosets

**Proposition-Definition 3.1** (Cosets). Let \(G\) be a group and let \(H \leq G\) be a subgroup. Define a relation \(\equiv_H\) on \(G\) by saying that for \(a, b \in G\) we have \(a \equiv_H b\) if \(b = ah\) for some \(h \in H\), that is, if \(a^{-1}b \in H\).

Then \(\equiv_H\) is an equivalence relation on \(G\).

The equivalence classes for this equivalence relation are called the left cosets of \(H\) in \(G\).

The cardinality of the quotient set \(G/\equiv_H\) is called the index of \(H\) in \(G\) and is denoted by \(\lvert G : H \rvert\).

Note that, by the above definition, if \(H \leq G\) and \(a \in G\), then the \(\equiv_H\)-class of \(a\) is exactly the set
\[
aH := \{ ah \mid h \in H \}
\]
The quotient set \(G/\equiv_H\) is also denoted by \(G/H\). Thus
\[
G/H = \{ [g]_{\equiv_H} \mid g \in G \} = \{ gh \mid g \in G \}.
\]

The following properties of cosets follow easily from the definition of a coset and from the fact that \(\equiv_H\) is an equivalence relation on \(G\):

**Proposition 3.2.** Let \(G\) be a group and let \(H \leq G\) be a subgroup. Then:

1. For \(a, b \in G\), if \(a^{-1}b \in H\) then \(aH = bH\), and if \(a^{-1}b \notin H\) then \(aH \cap bH = \emptyset\). In particular, if \(aH \neq bH\) then \(aH \cap bH = \emptyset\).
2. For every \(a \in G\) we have \(a \in aH\).
3. For every \(h \in H\) we have \(hH = e_G H = H\).
4. For an element \(a \in G\) we have \(aH = H\) if and only if \(a \in H\).

**Theorem 3.3.** Let \(G\) be a group and let \(H \leq G\) be a subgroup such that \(\lvert G : H \rvert = 2\). Then \(H \triangleleft G\).

*Proof.* Since \(\lvert G : H \rvert = 2\), we have \(\lvert G/H \rvert = 2\) and hence \(G/H = \{ e_G H, aH \} = \{ H, aH \}\) for some element \(a \in G \setminus H\). Therefore \(H \cap aH = \emptyset\) and \(G = H \cup aH\).

Let \(h \in H\) and let \(g \in G\) be arbitrary. We need to show that \(ghg^{-1} \in H\).

If \(g \in H\) then \(ghg^{-1} \in H\) since \(H \leq G\). Suppose now that \(g \notin H\). Since \(G = H \cup aH\), it follows that \(g \in aH\), so that \(g = ah_1\) for some \(h_1 \in H\).
Now consider the element $ghg^{-1} = ab_1hh_1^{-1}a^{-1}$. We claim that again $gh^{-1}g \in H$.

Indeed, suppose not, that is, suppose that $gh^{-1}g \notin H$. Then $ghg^{-1} \in aH$ so that $ghg^{-1} = ah$ for some $h \in H$. Thus $ah_1hh_1^{-1}a^{-1} = ah_2$. This implies that $h_1hh_1^{-1}a^{-1} = h_2$. Hence $h_2h_1hh_1^{-1} = e$ and therefore

$$h_2^{-1}h_1hh_1^{-1} = a.$$ 

Since $H \leq G$ and $h, h_1, h_2 \in H$, this implies that $a \in H$, contrary to the fact that $a \notin G - H$. Thus $gh^{-1}g \in H$.

We have verified that for all $g \in G, h \in H$ we have $ghg^{-1} \in H$, so that $H \triangleleft G$, as required.

\[ \Box \]

**Lemma 3.4.** Let $G$ be a group, let $H \leq G$, and let $a \in G$. Define a function $f_a : H \rightarrow aH$ by $f_a(h) = ah$ for $h \in H$.

Then $f_a : H \rightarrow aH$ is a bijection. In particular this implies that $|H| = |aH|$ for every $a \in G$.

**Theorem 3.5** (Lagrange). Let $G$ be a finite group and let $H \leq G$ be a subgroup. Then


In particular, $|H|||G|$.

**Proof.** Let $[G : H] = m$ and choose a transversal $T = \{g_1, \ldots, g_m\}$ for $\equiv_H$ in $G$. Then

$$G = g_1H \cup \cdots \cup g_mH$$ 

and $g_iH \cap g_jH = \varnothing$ for $i \neq j$. By Lemma 3.4 we have $|g_iH| = |H|$ for $i = 1, \ldots, m$. Therefore $|G| = m|H| = [G : H]|H|$, as required.

\[ \Box \]

**Corollary 3.6.** Let $G$ be a finite group and let $a \in G$. Then $\text{ord}(a)||G|$.

**Proof.** Put $H = \langle a \rangle \leq G$. Since $H$ is a finite set, Theorem 2.12 implies that $\text{ord}(a) = |H| < \infty$.

Theorem 3.5 now implies that $\text{ord}(a)||G|$.

\[ \Box \]

### 3.1. Additional problems.

1. Let $G_1, G_2$ be groups. Consider the set $G_1 \times G_2$ with the operation $\cdot$ defined as $(g_1, g_2) \cdot (g'_1, g'_2) = (g_1g'_1, g_2g'_2)$, where $g_1, g'_1 \in G_1$ and $g_2, g'_2 \in G_2$ are arbitrary. Prove that $(G_1 \times G_2, \cdot)$ is a group.

2. Let $G_1, G_2$ be groups and let $G = G_1 \times G_2$ be the group defined in (1). Let $H = \{(g_1, eg_2) | g_1 \in G_1 \}$ and $K = \{(eg_1, g_2) | g_2 \in G_2 \}$. Prove that $H \triangleleft G$ and $K \triangleleft G$.

3. Let $G_1, G_2$ be groups and let $G = G_1 \times G_2$ be the group defined in (1). Prove that $G$ is abelian if and only if $G_1$ and $G_2$ are both abelian.

4. Let $G_1, G_2$ be groups and let $G = G_1 \times G_2$ be the group defined in (1). Let $a \in G_1, b \in G_2$ be such that $\text{ord}(a) = m < \infty$ and $\text{ord}(b) = n < \infty$. Prove that for $g = (a, b) \in G$ we have $\text{ord}(g) = \text{lcm}(m, n)$. 

(5) Prove that if \( p, q \geq 2 \) are integers such that \( \gcd(p, q) = 1 \) then the group \( G = \mathbb{Z}_p \times \mathbb{Z}_q \) is cyclic. (Here \( \mathbb{Z}_p, \mathbb{Z}_q \) are groups with respect to addition). 

**Hint:** Take \( a = [1]_p \in \mathbb{Z}_p, b = [1]_q \in \mathbb{Z}_q \) and \( g = (a, b) \in G \). Use part (4) above to conclude that \( \text{ord}(g) = pq \). Then use the fact that \( \text{ord}(g) = |\langle g \rangle| \) and the fact that \( |G| = pq \) to conclude that \( G = \langle g \rangle \).