Chapter 6

Theory of groups

Main definitions

Def.: A nonempty set G with an operation $*$ defined in it, i.e. $(G, *)$, is called a group if

1. $*$ is associative: $a * (b * c) = (a * b) * c$
2. there exists a neutral element e: $a * e = e * a = a$
3. Each element has an inverse: $a^{-1} * a = a * a^{-1} = e$.

Def.: If $(G, *)$ is a group and the operation $*$ is commutative $(a * b = b * a)$, then G is called commutative or abelian group.

Def.: Given $(G, *)$ we will call the order of G the number of elements of G: $|G| = \mathrm{card}(G)$.

Def.: Given $g \in G$ we will call the order of g the number

$$\mathrm{ord}(g) = \min\{n\}, \quad \text{s.t.} \quad g^n = \underbrace{g * g * \cdots * g}_{n \text{ times}} = e$$

Problem 6.1a Show that $G = (\mathbb{R}\backslash\{0\}, \times)$ is a group.

Let's check the properties:

1. $a \times (b \times c) = (a \times b) \times c$. True
2. Neutral element $e = 1$, then $a \times 1 = 1 \times a = a$. True
3. Inverse element $a^{-1} = \frac{1}{a}$, then $a \times \frac{1}{a} = 1$. True

Problem 6.1b Show that $G = (\{1, -1, i, -i\}, \times)$ is a group.

Let's check the properties:

1. $a \times (b \times c) = (a \times b) \times c$. True (complex numbers)
2. Neutral element $e = 1$, then $a \times 1 = 1 \times a = a$. True
3. Inverse elements $1^{-1} = 1$, $(-1)^{-1} = -1$, $i^{-1} = -i$, and $(-i)^{-1} = i$. True

Problem 6.1f Orthogonal group.

$$O(2,\mathbb{Z}_3)=\left\{A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}:\ a,b,c,d\in\mathbb{Z}_3,\ \det(A)\neq 0,\ A^T=A^{-1}\right\}$$

with matrix product.

0. $AB\in O$. Indeed, $\det(AB)=\det(A)\det(B)\neq 0$. Inverse:

$$(AB)^{-1}=B^{-1}A^{-1}=B^TA^T=(AB)^T$$

1. Associativity is obvious
2. Neutral element: $e=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
3. Inverse: $A^{-1}=A^T$

Problem 6.2: Find why the following sets are not groups

a) $G = \{x \in \mathbb{R} : \ x < 0\}$ with the product. No neutral element.

b) $G = \{a \in \mathbb{Z} : a \text{ is a square}\}$ with the sum. No inverse (e.g. 4 and $-4 \notin G$).

d) $G = \{[0], [2], [3], [6]\} \subset \mathbb{Z}_8$ with the product. $[0]$ has no inverse.

Problem 6.4: Let $G = (\mathbb{R}, *)$. Find $*$ s.t. $x^{-1} = 1 - x$.

By definition $x * e = x$ and $x^{-1} * x = (1 - x) * x = e$.
Let's check a linear function: $x * y = ax + by + c$

$$ax + be + c = x, \quad ae + bx + c = x, \quad ax + b(1 - x) + c = e$$

Solving these equations we get: $a = b = 1$, $c = -e$. Then $e = \frac{1}{2}$ and we get the operation:

$$x * y = x + y - \frac{1}{2}$$

Subgroups

The algebraic structures usually have subsets that inherit the structure, e.g. vector spaces have vector subspaces.

Def.: Let $(G, *)$ be a group and S is a subset of G ($S \subset G$). We say that S with the operation $*$, i.e. $(S, *)$, is a subgroup of G if $(S, *)$ is a group.

Notation: We denote subgroups $S \trianglelefteq G$. If $|S| < |G|$ then $S \triangleleft G$.

Example 1: $\mathbb{Z} \triangleleft \mathbb{Q} \triangleleft \mathbb{R}$ with addition.

Example 2: From Problem 6.1b: $(\{1, -1, i, -i\}, \times)$ is a group. Then $(\{1, -1\}, \times)$ and $(\{1\}, \times)$ are subgroups.

Problem 6.5: Let $(G, *)$ be a group and $S \subset G$. Prove that H is a subgroup iff $\forall a, b \in S$ we have $a * b^{-1} \in S$.

1. The operation $*$ is associative in S since it is in G.
2. Neutral element: Let take $a = b$ then we have $a * a^{-1} = e \in S$.
3. Inverse: Taking $a = e$ we get $e * b^{-1} = b^{-1} \in S$. Finally, taking $b = b^{-1}$ we have $a * (b^{-1})^{-1} = a * b \in S$.

Problem 6.6: Let $(G, *)$ be a group and H is a finite subset, s.t. $\forall a, b \in H$ $a * b \in H$. Then H is a subgroup.

1. Associativity is straightforward.
2. Neutral element: Let $n = \mathrm{card} H$. Since $a_1 * a_2 * \cdots * a_n \in H$ then we have

$$a_1 * a_2 * \cdots * a_n = a_k \in H$$

We then can order elements such that $k = n$. Then

$$a_n = (a_1 * \cdots * a_{n-1}) * a_n = e * a_n$$

Thus, there exists the neutral element $e = a_1 * \cdots * a_{n-1}$. Note that $e \in G$ and it is also the neutral element of G. Thus $a_i * e = e * a_i = a_i$ for $i = 1, ..., n$.

3. Inverse:

$$e = a_1 * (a_2 * a_3 * \cdots * a_{n-1}) = a_1 * a_k, \quad a_k \in H$$

Thus, a_1 has an inverse in H. This then can be extended to all elements.

Def.: Let $(G, *)$ be a group and $X \subseteq G$. We denote by $< X >$ the subgroup generated by X corresponding to the smallest subgroup of G that contains X, i.e.,

$$< X >= \bigcap_{X \subset S \trianglelefteq G} S$$

A group that can be generated by a single element is called cyclic group.

$$< g >= G$$

Given $g \in G$, then every other element can be obtained by repeatedly applying the group operation or its inverse to g.

Examples: $(\mathbb{Z}, +)$: $< 1 >= \mathbb{Z}$; $< 2 >= 2\mathbb{Z}$
Observation: $< 2 >=< 4, 6 >$. Indeed, $4, 6 \in 2\mathbb{Z}$ thus $< 4, 6 >\subseteq< 2 >$, then $2 = 6 - 4$ and hence $2 \in< 4, 6 >$.

Let $(G, *)$ be a finite group and n be the order of g_i, i.e, $g_i^n = e$. Then $\{g_i, g_i^2, \dots, g_i^{n-1}, e\}$ forms a cyclic group.

If $(G, *)$ is a cyclic group and g is its generator, then $\mathrm{ord}(g) = |G|$.

Let S be a subgroup of G. Then $|S|$ divides $|G|$. Moreover, if $n = |G|$ and $m_i = \mathrm{ord}(g_i)$ then

$$m_i | n \quad i = 1, 2, \dots, n$$

Problem 6.7: Enumerate all elements of the linear group

$$GL(2, \mathbb{Z}_2) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \quad a, b, c, d \in \mathbb{Z}_2, \ ad - bc \neq_2 0 \right\}$$

and construct the table of operations.

$$g_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$g_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad g_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad g_6 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$\times$	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_1	g_6	g_5	g_4	g_3
g_3	g_3	g_5	g_1	g_6	g_2	g_4
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

elelment	g_1	g_2	g_3	g_4	g_5	g_6
$\mathrm{ord}(g_i)$	1	2	2	2	3	3

The group is neither Abelian ($g_2 \times g_3 = g_6 \neq g_5 = g_3 \times g_2$) nor cyclic: $\mathrm{ord}(g_i) < |G|$.

g_5 generates a cyclic subgroup S of G:

$$g_5^2 = g_6, \quad g_5^3 = g_1 = e \quad \Rightarrow \quad S = \{g_5, g_6, e\}$$

We can check: $g_6^2 = g_5$ and $g_5 g_6 = g_6 g_5 = e$.

Def.: The orthogonal group of order n, $O(n, F)$, is a group of orthogonal matrices $n \times n$ over the field F with the operation of matrix multiplication. $O(n, F) \lhd GL(n, F)$.

Def.: A square matrix M is orthogonal iff:

$$M * M^T = I \quad \Rightarrow \quad M^{-1} = M^T$$

Problem 6.8: Indicate the eight elements of the orthogonal group $O(2, \mathbb{Z}_3)$ and evaluate the table for this group. Find the orders of its elements and decide if it is abelian or cyclic.

$$g_i = \begin{pmatrix} [a]_3 & [b]_3 \\ [c]_3 & [d]_3 \end{pmatrix} \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$[a^2]_3 + [b^2]_3 = [1]_3, \quad [c^2]_3 + [d^2]_3 = [1]_3, \quad [ac]_3 + [bd]_3 = [0]_3$$

If $a = [0]$ then $b \in \{[1], [2]\}$ and $d = [0]$, and $c \in \{[1], [2]\}$. Thus

$$g_1 = \begin{pmatrix} [0] & [1] \\ [1] & [0] \end{pmatrix}, \quad g_2 = \begin{pmatrix} [0] & [1] \\ [2] & [0] \end{pmatrix},$$

$$g_3 = \begin{pmatrix} [0] & [2] \\ [1] & [0] \end{pmatrix}, \quad g_4 = \begin{pmatrix} [0] & [2] \\ [2] & [0] \end{pmatrix}.$$

If $a \in \{[1],[2]\}$ then $b=[0]$ and $c=[0]$, and $d \in \{[1],[2]\}$. Thus

$$g_5 = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}, \quad g_6 = \begin{pmatrix} [1] & [0] \\ [0] & [2] \end{pmatrix},$$

$$g_7 = \begin{pmatrix} [2] & [0] \\ [0] & [1] \end{pmatrix}, \quad g_8 = \begin{pmatrix} [2] & [0] \\ [0] & [2] \end{pmatrix}.$$

The multiplication table:

$\times$	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_1	g_5	g_7	g_6	g_8	g_1	g_3	g_2	g_4
g_2	g_6	g_8	g_5	g_7	g_2	g_4	g_1	g_3
g_3	g_7	g_5	g_8	g_6	g_3	g_1	g_4	g_2
g_4	g_8	g_6	g_7	g_5	g_4	g_2	g_3	g_1
g_5	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_6	g_2	g_1	g_4	g_3	g_6	g_5	g_8	g_7
g_7	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_8	g_4	g_3	g_2	g_1	g_8	g_7	g_6	g_5

The group is not abelian (e.g. $g_1 \times g_2 = g_7 \neq g_6 = g_2 \times g_1$).

Order of elements (in our case $e = g_5$:

$$g_1^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus order of g_1 is 2. Then similarly:

$$g_2^4 = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus, we get

g	1	2	3	4	5	6	7	8
order	2	4	4	2	1	2	2	2

Non of the element has the order 8, thus the group is not cyclic.

Problem 6.9. Find the order of elements of $\mathbb{Z}_n^*$ for $n = 6, 7, 8, 9$. Indicate the generator for each group.

$n = 6$: $\mathbb{Z}_6^* = \{1, 5\}$. $1^k = 1 \Rightarrow |1| = 1$; $[5^2] = [1]_6 \Rightarrow |5| = 2$; The generator is $< 5 >= \mathbb{Z}_6^*$

$n = 7$: $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

z_i	1	2	3	4	5	6
order	1	3	6	3	6	2

Thus, $< 3 >=< 5 >= \mathbb{Z}_7^*$

$n = 8$: $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$.

z_i	1	3	5	7
order	1	2	2	2

Thus, $< 3, 5 >= \mathbb{Z}_8^*$

$n = 9$: $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$.

z_i	1	2	4	5	7	8
order	1	6	3	6	3	2

Thus, $< 2 >=< 5 >= \mathbb{Z}_8^*$

Cartesian product of groups

Def.: Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. We consider their cartesian product

$$G = G_1 \times G_2$$

and define the operation over the product:

$$\begin{array}{rcl} * : \; G & \to & G \\ ((g_1, g_2), (h_1, h_2)) & \mapsto & (g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2) \end{array}$$

Then $G = G_1 \times G_2 = G_1 \oplus G_2$ is called the direct product of groups.

Theorem: $G_1 \oplus G_2$ is a group.

Example. As $30 = 2 \times 3 \times 5$, earlier we have seen that the group $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, +)$ is equivalent to $(\mathbb{Z}_{30}, +)$. There exists a bijection between these groups that conserves the operation $+$.

Homomorphism of groups

Def.: Given two groups $(G_1, *_1)$ and $(G_2, *_2)$ and a map:

$$T : \ (G_1, *_1) \to (G_2, *_2)$$

We then say that T is a homomorphism if $\forall g, h \in G_1$ we have

$$T(g *_1 h) = T(g) *_2 T(h).$$

(i.e., the map preserves the operation).

We also say that T is

1. a monomorphism if T is an injective homomorphism
2. an epimorphism if T is a surjective homomorphism
3. an isomorphism if T is a bijective homomorphism

Problem 6.10: Find explicitly a group isomorphism $\mathbb{Z}_{12} \times \mathbb{Z}_{11} \to \mathbb{Z}_{132}$.

11 and 12 are coprimes and $11 \times 12 = 132$. Then we introduce:

$$\begin{array}{rcl} T: \ (\mathbb{Z}_{132}, +) & \to & (\mathbb{Z}_{12} \times \mathbb{Z}_{11}, +) \\ [a]_{132} & \mapsto & T([a]_{132}) = ([a]_{12}, [a]_{11}) \end{array}$$

Now for $a, b \in \mathbb{Z}_{132}$ we have

$$T([a]_{132} + [b]_{132}) = T([a+b]_{132}) = ([a+b]_{12}, [a+b]_{11}) =$$

$$= ([a]_{12}, [a]_{11}) + ([b]_{12}, [b]_{11}) = T([a]_{132}) + T([b]_{132})$$

Thus T is a homomorphism. Besides, the Chinese theorem says that T is a bijection. Therefore, T is an isomorphism between the groups. Then, the inverse operation is an isomorphism:

$$T^{-1} : \mathbb{Z}_{11} \times \mathbb{Z}_{12} \to \mathbb{Z}_{132}$$

$$([a]_{11},[b]_{12}) \mapsto [a\times 12\times [12]_{11}^{-1}+b\times 11\times [11]_{12}^{-1}]_{132} = [12a+121b]_{132}$$

Problem 6.11: Let G be a group and $a, b \in G$. Prove that
(a) if $\mathrm{ord}(a) = n$ and $n = pq$, then $\mathrm{ord}(a^p) = q$.

First we note that $a^p \in G$. Then

$$\mathrm{ord}(a) = n \;\Rightarrow\; a^n = e \;\Rightarrow\; a^{pq} = (a^p)^q = e \;\Rightarrow\; \mathrm{ord}(a^p) = q$$

(b) $\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$.

Let $\mathrm{ord}(a) = n$. Then

$$a^{-1} * a = e \;\Rightarrow\; a^{-1} * a^{-1} * a * a = a^{-1} * e * a = e$$

Thus

$$e = (a^{-1})^n * a^n = (a^{-1})^n * e = (a^{-1})^n \;\Rightarrow\; \mathrm{ord}(a^{-1}) = n$$

(c) If a, b are commutative and have finite orders that are coprimes then $< a > \cap < b >= \{e\}$.

$$< a >= \{a^k : \ k = 1, \ldots, n\}, \quad < b >= \{b^k : \ k = 1, \ldots, m\}$$

It is obvious that $e \in< a >$ and $e \in< b >$. Now let's assume that there exists $u \in< a >$ and $u \in< b >$ then

$$u = a^i = b^j \ \Rightarrow \ u^n = a^{in} = (a^n)^i = e = b^{jn}$$

Thus $m|jn$, but since $\gcd(m, n) = 1$ then $m|j$ and $u = b^j = e$.

Quaternions

This is an extension of the complex numbers. It is defined by introducing i, j, k, s.t. $i^2 = j^2 = k^2 = ijk = -1$.
Then a quaternion number is given by:

$$x = a + bi + cj + dk \in \mathbb{H}$$

To get the table of multiplication we observe, e.g.:

$$i^2jk = -i \Rightarrow jk = i \Rightarrow j^2k = ji \Rightarrow ji = -k \Rightarrow ji^2 = -ki \Rightarrow ki = j$$

$\times$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Problem 6.12: Quaternion group

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\; i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\; j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\; k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Show that $G = \{1, -1, i, -i, j, -j, k, -k\}$ is a group with matrix product.

The associative property is obvious. The neutral element $e = 1$. To find the inverse we build the multiplication table (and also check that all products belong to G). For simplicity only the main 4 elements are considered. Note

×	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

The inverses: $1 \times 1 = 1$, $-i \times i = 1$, $-j \times j = 1$, and $-k \times k = 1$.

element	1	i	j	k	-1	$-i$	$-j$	$-k$
order	1	4	4	4	2	4	4	4

The group is neither Abelian nor cyclic.
Problem 6.14: Prove that $|G|$ is a prime number iff G has no proper subgroups, i.e., $\{e\}$ and $\{G\}$ are the only subgroups of G.

Let $p = |G|$ be a prime and S be a subgroup of G. Then by the Lagrange theorem $|S|$ divides p, i.e., $|S| \in \{1, p\}$. Thus, S is either $\{e\}$ or G.

Let now $a \in G$ and $a \neq e$. Then $\langle a \rangle = G$ (since G has no other subgroups). Thus, $G = \{a, a^2, \ldots, a^{n-1}, e\}$ is cyclic. If n is not prime, then $n = qp$ and $e = a^n = a^{qp} = (a^q)^p$. Thus, a^q generates a subgroup of order $1 < p < n$, which contradicts the assumption.

Problem 6.15: Prove that if $|G|$ is a prime number then G is cyclic.

Let $|G| = p$. Then $\mathrm{ord}(g_i)|p$, i.e. $\mathrm{ord}(g_i) \in \{1, p\}$. If $\mathrm{ord}(g_j) = 1$ then $g_j = e$. Therefore there exists at least one element ($p \geq 2$) s.t. $\mathrm{ord}(g_k) = p$. Then $< g_k >= G$ and the group is cyclic.

Problem 6.17: Prove:
(a) If p and n are coprimes, then there exists $m \geq 1$ s.t. $n|p^m - 1$.

We have to prove that $[p^m - 1]_n = [0]_n$ or $[p^m]_n = [1]_n$.

The last equality is provided by the Little Fermat Theorem: $p^{\phi(n)} \equiv 1 \bmod n$. Thus, we can take $m = \phi(n) \geq 1$.

(b) If p and n are primes ($p \neq n$), then $n|p^{n-1} - 1$.

Again we use the theorem: $[p^{\phi(n)}]_n = [1]_n$. Then we note that $\phi(n) = n - 1$.

Classification of cyclic groups

The group $(\mathbb{Z}_n, +)$ is cyclic ($\mathbb{Z}_n =< [1]_n >$). Indeed:

$$[1]_n + [1]_n = [2]_n, \quad [2]_n + [1]_n = [3]_n, \ \ldots, \ [n-1]_n + [1]_n = [0]_n$$

Theorem: Any cyclic group $(G, *)$ of order n is isomorphic to $(\mathbb{Z}_n, +)$.

Proof: Since $G = \{g, g^2, \ldots, g^n\}$ we can introduce the map:

$$\begin{array}{rcl} T : (\mathbb{Z}_n, +) & \to & (G, *) \\ [i]_n & \mapsto & T([i]_n) = g^i \end{array}$$

T is an isomorphism.

Any cyclic group is Abelian (due to: $(\mathbb{Z}_n, +)$ is Abelian).

Theorem: The group $(\mathbb{Z}_m \times \mathbb{Z}_k, +)$ is cyclic iff $\gcd(m, k) = 1$.

This follows from the Chinese theorem and the map

$$T : (\mathbb{Z}_{m\times k}, +) \to (\mathbb{Z}_m \times \mathbb{Z}_k, +)$$

Example: $(\mathbb{Z}_{12} \times \mathbb{Z}_5, +)$ is cyclic and isomorphic to $(\mathbb{Z}_{60}, +)$.
However, $(\mathbb{Z}_{10} \times \mathbb{Z}_6, +)$ is not cyclic since $\gcd(10, 6) = 2$.

In general: For $n \in \mathbb{N}\backslash\{0\}$ we have $n = p_1^{r_1} \cdots p_k^{r_k}$. Then the group

$$\left(\bigoplus_{i=1}^{k} \mathbb{Z}_{p_k^{r_k}}, + \right)$$

is isomorphic to $(\mathbb{Z}_n, +)$.

Problem 6.19: Let $G_1 = \mathbb{Z}_{24} \times \mathbb{Z}_{60}$ and $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_{20}$ be two additive groups.
(a) Show that G_1 and G_2 are not isomorphic.

First we note that the order of G_1 and G_2 is the same:
$|G_1| = 24 \times 60 = 1440 = 2 \times 6 \times 6 \times 20 = |G_2|$.

Now we can develop into primes: $24 = 3 \times 8$ thus $\mathbb{Z}_{24} \cong \mathbb{Z}_3 \times \mathbb{Z}_8$

The same way: $60 = 3 \times 4 \times 5$ and $\mathbb{Z}_{60} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$

Thus we have an isomorphism:

$$G_1 \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_8$$

whereas: $G_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$

Therefore G_1 and G_2 are not isomorphic ($\mathbb{Z}_8$ is cyclic, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is not).

(b) Search for surjective (onto) homomorphisms of G_1 or G_2 over $\mathbb{Z}_{120}$

Note that $< [1]_{120} >= \mathbb{Z}_{120}$. Let

$$\begin{array}{rcl} f : \mathbb{Z}_{24} \times \mathbb{Z}_{60} & \to & \mathbb{Z}_{120} \\ (x, y) & \mapsto & f(x, y) = z \end{array}$$

f is surjective, i.e. $\forall z \, \exists (x, y)$ s.t. $f(x, y) = z$. f is homomorphism:

$$f((x_1, y_1) + (x_2, y_2)) = f(x_1, y_1) + f(x_2, y_2)$$

Thus, we search for a cyclic subgroup H of G_1, s.t. $|H| = 120$. Then we can have

$$\mathbb{Z}_{24} \times \mathbb{Z}_{60} \to \mathbb{Z}_{120} \times \mathbb{Z}_{12} \to \mathbb{Z}_{120}$$
$$([x]_{24}, [y]_{60}) \mapsto (u, v) \mapsto z = (u, 0)$$

The first map is an isomorphism:

$$G_1 \cong \mathbb{Z}_3 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{120} \times \mathbb{Z}_{12}$$

We have $[y]_{60} \mapsto ([y]_5, [y]_{12})$ and hence

$$\begin{aligned} u &\equiv x \mod 24 \\ u &\equiv y \mod 5 \end{aligned}$$

$q_1 = 5,\ r_1 = [5]_{24}^{-1} = [5]_{24}$ and $q_2 = 24,\ r_2 = [24]_5^{-1} = [-1]_5$ hence

$$u = [25x - 24y]_{120}$$

Whereas the second map is surjective homomorphism

$$z = [25x - 24y]_{120}$$

Thus, $G_1 \ni ([x]_{24}, [y]_{60}) \mapsto z = T(x, y) = [25x - 24y]_{120} \in \mathbb{Z}_{120}$

(c) Find 4 groups not isomorphic to G_1 and G_2.

The groups orders cannot be reducible to those shown in (a), e.g. $\mathbb{Z}_3 \times \mathbb{Z}_{480} \cong G_1$

1. $\mathbb{Z}_{1440}$ is cyclic.
2. $\mathbb{Z}_{10} \times \mathbb{Z}_{144} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_{16} \times \mathbb{Z}_9$.
3. $\mathbb{Z}_{48} \times \mathbb{Z}_{30} \cong \mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
4. $\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5$