1 Groups

Definition 1.1. Let G be a non empty set. We define a grouop as a pair $(G, *)$ where $*$ is a binary operation

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (g_1, g_2) &\longmapsto g_1 * g_2 \end{aligned} \tag{1}$$

such that the following properties are satisfied.

1. Associativity: $(xy)z = x(yz)\ \forall x, y, z \in G$
2. Identity element: $\forall x \in G\ \exists e \in G$ such that $eg = ge = g$
3. Inverse element: $\forall x \in G\ \exists x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = e$

Definition 1.2. Let $(G, *)$ be a group. We say G is *commutative* or *abelian* if and only if

$$\forall g_1, g_2 \in G,\ g_1 g_2 = g_2 g_1. \tag{2}$$

Lemma 1.1. *Let $(G, *)$ be a group. Then,*

1. *The identity element is unique*
2. *The inverse element of $g \in G$ is unique.*
3. *Given $g, h \in G$ such that $gh = e$, then $h = g^{-1}$*
4. *Given $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$*
5. *Given $g, u, v \in G$ such that $gu = gv$, then $u = v$*
6. *Given $g, u, v \in G$ such that $ug = vg$, then $u = v$*
7. *Given $g \in G$, $(g^{-1})^{-1} = g$.*

Corollary 1.2. *Let $\varphi : G \longrightarrow$ be an application defined by $\varphi(g) = g^{-1}$. Then,*

1. $\varphi^2 = \mathrm{id}_G$
2. $\varphi(g_1 * g_2) = \varphi(g_2) * \varphi(g_1)$.

Definition 1.3. Let $(G, *)$ be a group and $H \subseteq G$ a subset of G. We say $(H, *)$ is a *subgroup* of $(G, *)$ if and only if

1. $h_1, h_2 \in H \Rightarrow h_1 * h_2 \in H$.
2. $e_G \in H$.
3. $h \in H \Rightarrow h^{-1} \in H$.

Proposition 1.3. *Let $(G, *)$ be a group and $H \subseteq G$ a subset of G. Then,*

1. *$(H.*)$ is a subgroup of $(G, *)$ if and only if $H \neq \emptyset$ and $\forall h_1, h_2 \in H$, $h_1 * h_2^{-1} \in H$.*
2. *$(H.*)$ is a subgroup of $(G, *)$ if and only if $H \neq \emptyset$ and $\forall h_1, h_2 \in H$, $h_1^{-1} * h_2 \in H$.*

Proposition 1.4. *Let $(H, *)$ be a subgroup of $\mathbb{Z}, +)$. Then there exists a number $n \in \mathbb{Z}$ such that $H = n\mathbb{Z}$.*

Proposition 1.5. *Let $(G_i, *_i)$ with $i = 1, \dots, n$ be n groups. Then, the product $G_1 \times \cdots \times G_n$ induces a group with the operation defined as*

$$(g_1, \dots, g_n) *' (g'_1, \dots, g'_n) := (g_1 * g'_1, \dots, g_n * g'_n). \tag{3}$$

Definition 1.4. Let $(G, *)$ be a group. We define the *order* of G as the number $|G|$ of elements in G.

Lemma 1.6. *Let $(G, *)$ be a group and $(H_i, *)_I$ a collection of subgroups of $(G, *)$. Then, the set*

$$H := \bigcap_{i \in I} H_i \tag{4}$$

is a subgroup of $(G, *)$.

Definition 1.5. Let $(G, *)$ be a group and $X \subseteq G$ a subset of G. We define the *subgroup generated* by X as the smallest subgroup $(\langle X \rangle, *)$ that contains X.

Proposition 1.7. *Let $(G, *)$ be a subgroup and $X \subseteq G$ a subset of G. Then, the sbugroup $(\langle X \rangle, *)$ generated by X is determiend by*

$$\langle X \rangle = \bigcap_{H \leq G, X \subseteq H} H. \tag{5}$$

Definition 1.6. Let $(G, *)$ be a group, $g \in G$ an element and $n \in \mathbb{Z}$ a number. We define the *n-th power* of g as

$$g^n := \begin{cases} g * \cdots g & n > 0 \\ e & n = 0 \\ g^{-1} * \cdots * g^{-1} & n < 0 \end{cases}. \tag{6}$$

Lemma 1.8. *Let $(G, *)$ be a group and $g \in G$ an element. Then, for all $n, m \in \mathbb{Z}$ it is satisfied*

$$g^n * g^m = g^{n+m} = g^m * g^n. \tag{7}$$

Definition 1.7. Let $(G, *)$ be a group. We say $(G, *)$ is *cyclic* if and only if it is generated by one element.

Proposition 1.9. *Let $(G, *)$ b e a group and $g \in G$ an element. Then,*

$$\langle g \rangle = \bigcup_{i \in \mathbb{Z}} g^i \tag{8}$$

Definition 1.8. Let $(G, *)$ be a group and $g \in G$ an element. We define the *order* of g as the number of elements of $\langle g \rangle$.

Proposition 1.10. *$(\mathbb{Z}, +)$ is a cyclic group generated by $1 \in \mathbb{Z}$ and all subgroups of $(\mathbb{Z}, +)$ are cyclic.*

Proposition 1.11. *Let $(G, *)$ be a group and $g \in G$ an element. If $\operatorname{ord} g \neq |G|$, then $(G, *)$ is not cyclic.*

Proposition 1.12. *Let $(G, *)$ be a cyclic group. Then, $(G, *)$ is abelian.*

Proposition 1.13. *Let $(G, *)$ be a group and $g \in G$ an element. Then, $\operatorname{ord} g < \infty$ if and only if there exists a $n \in \mathbb{Z}^*$ such that $g^n = e$.*

Proposition 1.14. *Let $(G, *)$ be a group and $g \in G$ an element. Then,*

$$\operatorname{ord} g = \min \left\{ i > 0 \,\middle|\, g^i = e \right\}. \tag{9}$$

If no such i exists, we say $\operatorname{ord} g = \infty$

Corollary 1.15. *Let $n \in \mathbb{N}_{>1}$ a number and $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Then,*

$$\operatorname{ord} \bar{a} = \frac{n}{\gcd(a,n)} = \frac{\operatorname{lcm}(a,n)}{a}. \tag{10}$$

Corollary 1.16. *Let $\{(G_i, *_i)\}$ be a set of n group and $g_i \in G_i$ an element of each group to form $g = (g_1, \dots, g_n) \in G_1 \times \cdots \times G_n$. Then,*

$$\operatorname{ord} g = \operatorname{lcm}(\operatorname{ord} g_1, \dots, \operatorname{ord} g_n). \tag{11}$$

Corollary 1.17. *Let $(G_1, *_1), (G_2, *_2)$ be two cyclic groups. Then, $G_1 \times G_2$ induces a cyclic group if and only if $\gcd(\operatorname{ord} G_1, \operatorname{ord} G_2) = 1$, that is, $\operatorname{ord} G_1$ and $\operatorname{ord} G_2$ are coprime.*

Proposition 1.18. *Let $(G, *)$ be a cyclic group of order n and g its generator. Then,*

1. $g^m = e \Leftrightarrow n \mid m$
2. $g^a = g^b \Leftrightarrow a = b \mod n$
3. *If $0 \leq mleqn$, then $g^{-m} = (g^m)^{-1} = g^{n-m}$*

Proposition 1.19. *Let $(G, *)$ be a group and $F \subseteq G$ a subset of G. Then,*

$$\langle F \rangle = \{e\} \cup \{g_1^{\alpha_1} * \cdots g_n^{\alpha_n} \mid n \in \mathbb{N}, \alpha_i \in \mathbb{Z}, g_i \in F\}. \tag{12}$$

Theorem 1.20. *Every permutation is product of transposition. In particular, the symmetric group S_n is generated by*

$$S_n = \langle (1,2), \dots, (1,n) \rangle. \tag{13}$$

Theorem 1.21. *Let K be a field and $GL_n(K)$ the linear group. Every invertibe matrix of $GL_n(K)$ is product of elemental matrices. In other words, $GL_n(K)$ is generated by elemental matrices.*