3. Subgroups

Definition. Let G be a group. A non-empty set $H \subseteq G$ is a **subgroup** of G if for all $x, y \in H$, $x\,y^{-1} \in H$.

Notation. If H is a subgroup of G, then we write $H \leqslant G$. If $H \neq G$ is a subgroup of G, then we write $H < G$ and call H a **proper subgroup** of G.

Proposition 3.1. If $H \leqslant G$, then H is a group.

Proof. We have to show that H satisfies (A0), (A1), and (A2):

(A1) Let $x \in H$, then by definition, $x\,x^{-1} = e \in H$, so, the neutral element $e \in H$.
(A2) Let $x \in H$, then by definition $e\,x^{-1} = x^{-1} \in H$.
(A0) Let $x, y \in H$, then also $y^{-1} \in H$, and by definition $x(y^{-1})^{-1} = xy \in H$.

⊣

Definition. The subgroups $\{e\}$ and G are called the **trivial subgroups** of G.

Proposition 3.2. The intersection of arbitrarily many subgroups of a group G is again a subgroup of G.

Proof. Let Λ be any set and assume that for every $\lambda \in \Lambda$, $H_\lambda \leqslant G$. Let

$$H = \bigcap_{\lambda \in \Lambda} H_\lambda\,,$$

and take any $x, y \in H$. Then, for every $\lambda \in \Lambda$, $x, y \in H_\lambda$, and thus, for every $\lambda \in \Lambda$, $x\,y^{-1} \in H_\lambda$. Thus, $x\,y^{-1} \in H$, and since $x, y \in H$ were arbitrary, $H \leqslant G$. ⊣

Definition. Let G be a group with neutral element e and let $x \in G$. Then the least positive integer n such that $x^n = e$ is called the **order of** x, denoted by $\operatorname{ord}(x)$. If there is no such integer, then the order of x is "∞".

The order of an element x of a finite group G is well-defined: Because the set $\{x^1, x^2, x^3, \dots\} \subseteq G$ is finite, there are $0 < n < m$ such that $x^n = x^m = x^n\,x^{m-n}$, which implies $e = x^{m-n}$, where $m - n$ is a positive integer.

Definition. For a group G and a set $X \subseteq G$, let

$$\big\langle X \big\rangle := \bigcap_{\substack{H \leqslant G \\ X \subseteq H}} H\,.$$

By Proposition 3.2, $\big\langle X \big\rangle$ is a subgroup of G and it is called the subgroup **generated by** X. If $X = \{x\}$, then we write just $\langle x \rangle$ instead of $\big\langle \{x\} \big\rangle$.

Fact 3.3. If G is a group and $x \in G$ of order n, then $\langle x \rangle$ is a cyclic group (*i.e.*, subgroup of G) of order n.

Proof. The group $\langle x \rangle$ consists of the elements $x^1, x^2, \dots, x^n$, where $x^n = e$. On the other hand, $\{x^1, x^2, \dots, x^n\}$ is a cyclic group of order n. ⊣

This leads to the following:

Corollary 3.4. Let G be a group. If $x \in G$ is of finite order, then $\operatorname{ord}(x) = |\langle x \rangle|$.

Theorem 3.5. Subgroups of cyclic groups are cyclic.

Proof. Let $C_n = \{a^0, a^1, \ldots, a^{n-1}\}$ be a cyclic group of order n (for some positive integer n) and let $H \leqslant C_n$. If $H = \{a^0\}$, then we are done. So, let us assume that $a^m \in H$, where $m \in \{1, \ldots, n-1\}$. Take the least such m. Evidently, we have $\langle a^m \rangle \leqslant H$. Now, let $h \in H$ be arbitrary. Since $h \in C_n$, there is a $k \in \{0, 1, \ldots, n-1\}$ such that $h = a^k$. Write k in the form $k = \ell m + r$, where $\ell, r \in \mathbb{N}$ and $0 \leq r < m$. Now,

$$\underbrace{(a^m)^{-1} \cdots (a^m)^{-1}}_{\ell\text{-times}} = (a^m)^{-\ell} \in H\,,$$

and therefore, $h(a^m)^{-\ell} = a^k(a^m)^{-\ell} = a^r \in H$. Thus, by the choice of m, we must have $r = 0$, which implies that $h \in \langle a^m \rangle$. Since $h \in H$ was arbitrary, this implies $H \leqslant \langle a^m \rangle$ and completes the proof. ⊣

Definition. For $H \leqslant G$ and $x \in G$, let

$$xH := \{xh : h \in H\} \qquad \text{and} \qquad Hx := \{hx : h \in H\}\,.$$

The sets xH and Hx are called **left cosets** and **right cosets** of H in G (respectively).

In the sequel, left and right cosets will play an important role and we will use the following lemma quite often.

Lemma 3.6 (left-version). Let G be a group, $H \leqslant G$ and let $x, y \in G$ be arbitrary.
(a) $|xH| = |H|$, in other words, there exists a bijection between H and xH.
(b) $x \in xH$.
(c) $xH = H$ if and only if $x \in H$.
(d) $xH = yH$ if and only if $x^{-1}y \in H$.
(e) $xH = \{g \in G : gH = xH\}$.

Proof. (a) Define the function $\varphi_x : H \to xH$ by stipulating $\varphi_x(h) := xh$. We have to show that φ_x is a bijection. If $\varphi_x(h_1) = \varphi_x(h_2)$ for some $h_1, h_2 \in H$, *i.e.*, $xh_1 = xh_2$, then $xh_1h_2^{-1} = xh_2h_2^{-1} = xe = x$, which implies $h_1h_2^{-1} = e$, and consequently, $h_1 = h_2$. Thus, the mapping φ_x is injective (*i.e.*, one-to-one). On the other hand, every element in xH is of the form xh (for some $h \in H$), and since $xh = \varphi_x(h)$, the mapping φ_x is also surjective (*i.e.*, onto), thus, φ_x is a bijection between H and xH.

(b) Since $e \in H$, $xe = x \in xH$.

(c) If $xH = H$, then, since $e \in H$, $xe = x \in H$. For the other direction assume that $x \in H$: Because H is a group we have $xH \subseteq H$. Further, take any element $h \in H$. Since $x^{-1} \in H$ we have $x^{-1}h \in H$ and therefore $xH \ni x(x^{-1}h) = h$, which implies $xH \supseteq H$. Thus, we have $xH \subseteq H \subseteq xH$ which shows that $xH = H$.

(d) If $xH = yH$, then

$$\underbrace{x^{-1}xH}_{=H} = x^{-1}yH \overset{\text{by (c)}}{\Longrightarrow} x^{-1}y \in H\,.$$

If $x^{-1}y \in H$, then by (c) we have $x^{-1}yH = H$, and therefore, $\underbrace{xx^{-1}yH}_{yH} = xH$.

(e) If $g \in xH$, then $g = xh$ for some $h \in H$, and hence, $gH = xhH = xH$. Therefore, $xH \subseteq \{g \in G : gH = xH\}$. Conversely, if $xH = gH$ for some $g \in G$, then by (b), $g \in xH$, which implies $\{g \in G : gH = xH\} \subseteq xH$ and completes the proof. ⊣

Obviously, there exists also a right-version of Lemma 3.6, which is proved similarly. As a consequence of Lemma 3.6 (b), combining left-version and right-version, we get:

Corollary 3.7. Let $H \leqslant G$, then

$$\bigcup_{x \in G} xH = G = \bigcup_{x \in G} Hx\,.$$

The following lemma is a consequence of Lemma 3.6 (d):

Lemma 3.8 (left-version). Let $H \leqslant G$, then for any $x, y \in G$ we have either $xH = yH$ or $xH \cap yH = \emptyset$.

Proof. Either $xH \cap yH = \emptyset$ (and we are done) or there exists a $z \in xH \cap yH$. If $z \in xH \cap yH$, then $z = xh_1 = yh_2$ (for some $h_1, h_2 \in H$), thus, $x^{-1}z \in H$ and $z^{-1}y \in H$. Since H is a group, we get $(x^{-1}z)(z^{-1}y) = x^{-1}y \in H$, which implies by Lemma 3.6 (d) that $xH = yH$. ⊣

Obviously, there exists also a right-version of Lemma 3.8, which is proved similarly.

Definition. For a subgroup $H \leqslant G$ let

$$G/H := \{xH : x \in G\} \quad \text{and} \quad H\backslash G := \{Hx : x \in G\}\,.$$

Definition. A **partition** of a set S is a collection of pairwise disjoint non-empty subsets of S such that the union of these subsets is S.

As a consequence of Lemma 3.6 (a), Corollary 3.7 and Lemma 3.8 (left-versions and right-versions) we get:

Corollary 3.9. Let $H \leqslant G$, then G/H as well as $H\backslash G$ is a partition of G, where each part has the same order as H.

Definition. Let $H \leqslant G$, then $|G/H| = |H\backslash G|$ is called the **index** of H in G and is written $|G : H|$.

As a consequence of Corollary 3.9 we get:

Corollary 3.10. Let G be a group and let $H \leqslant G$. If $|G : H| = 2$, then for all $x \in G$ we have $xH = Hx$.

Proof. If $x \in H$, then $xH = Hx = H$ (since H is a group). Now, let $x \in G$ be not in H. By Corollary 3.9 we have $G = H \cup xH$ and $G = H \cup Hx$, where $H \cap xH = \emptyset = H \cap Hx$, which implies $xH = Hx$. ⊣

If $H \leqslant G$, then in general we do not have $xH = Hx$ (for all $x \in G$). For example, let C be the cube-group and let D_4 be the dihedral group of degree 4. It is easy to see that $D_4 \leqslant C$ and that the index of D_4 in C is 3. Now, holding a cube in your hand, it should not take too long to find a rotation $\rho \in C$ such that $\rho D_4 \neq D_4\rho$.

Theorem 3.11. Let G be a (finite) group and let $H \leqslant G$, then $|G| = |G : H| \cdot |H|$. In particular, for finite groups we get $|H|$ divides $|G|$.

Proof. Consider the partition G/H of G. This partition has $|G : H|$ parts and each part has size $|H|$ (by Lemma 3.6 (a)), and thus, $|G| = |G : H| \cdot |H|$. In particular, if $|G|$ is finite, $|H|$ divides $|G|$. ⊣

Corollary 3.12. If G is a finite group of order p, for some prime number p, then G is a cyclic group. In particular, G is abelian.

Proof. For every $x \in G$, $\langle x \rangle$ is a subgroup of G, hence, by Theorem 3.11, $|\langle x \rangle|$ divides $p = |G|$, which implies $|\langle x \rangle| = 1$ or $|\langle x \rangle| = p$. Now, $|\langle x \rangle| = 1$ iff $x = e$. So, if $x \neq e$, then $|\langle x \rangle| = p$, which implies $\langle x \rangle = G$. Hence, G is cyclic, and since cyclic groups are abelian, G is abelian. ⊣

Definition. A **transversal** for a partition is a set which contains exactly one element from each part of the partition. For $H \leqslant G$, a transversal for the partition G/H $(H\backslash G)$ is called a **left (right) transversal** for H in G.

For example, let $G = (\mathbb{C}^*, \cdot\,)$ and $H = (\mathbb{U}, \cdot\,)$, where $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$. First notice that the set $\mathbb{C}^*/\mathbb{U}$ consists of concentric circles. So, an obvious (left or right) transversal for $\mathbb{U}$ in $\mathbb{C}^*$ is $\mathbb{R}^+$, which is even a subgroup of $\mathbb{C}^*$. Another (left or right) transversal for $\mathbb{U}$ in $\mathbb{C}^*$ is $\mathbb{R}^- = \{x \in \mathbb{R} : x < 0\}$, which is not a subgroup of $\mathbb{C}^*$, but there are many other choices of transversals available.

If H is a subgroup of G and $x \in G$, then, as we have seen above, in general $xH \neq Hx$. This implies that a left transversal for H in G is not necessarily also a right transversal. However, by Lemma 3.6, it is straightforward to transform a left transversal into a right transversal:

Proposition 3.13. Let $H \leqslant G$ and let $\{a_0, a_1, \dots\}$ be a left transversal for H in G, then $\{a_0^{-1}, a_1^{-1}, \dots\}$ is a right transversal for H in G.

Proof. Let x and y be two distinct elements of $\{a_0, a_1, \dots\}$. Since $\{a_0, a_1, \dots\}$ is a left transversal for H in G, we have $xH \neq yH$, and by Lemma 3.6 (left and right version) we get:

$$x^{-1}y \notin H \iff (x^{-1}y)^{-1} \notin H \iff y^{-1}x \notin H \iff$$
$$\iff H \neq Hy^{-1}x \iff Hx^{-1} \neq Hy^{-1}\,.$$

Hence, $xH \neq yH$ if and only if $Hx^{-1} \neq Hy^{-1}$, and since x and y were arbitrary, this shows that $\{a_0^{-1}, a_1^{-1}, \dots\}$ is a right transversal for H in G. ⊣