Chapter 2. Subgroups

2.1 Definition: A **subgroup** of a group G is a subset $H \subseteq G$ which is also a group using the same operation as in G. When H is a subgroup of G, we write $H \leq G$.

2.2 Example: In any group G we have the subgroups $\{e\} \leq G$ and $G \leq G$. The group $\{e\}$ is called the **trivial** group. A subgroup $H \leq G$ with $H \neq G$ is called a **proper** subgroup of G.

2.3 Example: We have $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$. and we have $\mathbb{Z}^* \leq \mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$.

2.4 Example: Note that $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ is not a subgroup of $\mathbb{Z}$, indeed it is not even a subset. Also, U_n is not a subgroup of $\mathbb{Z}_n$ since it uses a different operation.

2.5 Theorem: (*The Subgroup Test I*) *Let G be a group and let $H \subseteq G$. Then $H \leq G$ if and only if*

(1) H contains the identity, that is $e \in H$,
(2) H is closed under the operation, that is $ab \in H$ for all $a, b \in H$, and
(3) H is closed under inversion, that is $a^{-1} \in H$ for all $a \in H$.

Proof: Note first that the operation on the group G restricts to a well defined operation on H if and only if H is closed under the operation. In this case, the operation will be associative on H since it is associative on G. Next note that if $e = e_G \in H$ then e is an identity element for H, and conversely if e_H is an identity for H then since $e_H e_H = e_H$ (both in H and in G), cancellation in the group G gives $e_H = e_G$. Thus H has an identity if and only if $e_H = e_G \in H$. A similar argument shows that a given element $a \in H$ has an inverse in H if and only if $a^{-1} \in H$ where a^{-1} denotes the inverse of a in G.

2.6 Theorem: (*The Subgroup Test II*) *Let G be a group and let $H \subseteq G$. Then $H \leq G$ if and only if*

(1) $H \neq \emptyset$, and
(2) for all $a, b \in H$ we have $ab^{-1} \in H$.

Proof: From the Subgroup Test I, it is clear that if $H \leq G$ then (1) and (2) hold. Suppose, conversely, that (1) and (2) hold. By (1) we can choose an element $a \in H$, and then by (2) we have $e = aa^{-1} \in H$, so H contains the identity. For $a \in H$, we have $a^{-1} = ea^{-1} \in H$ by (2), so H is closed under inversion. For $a, b \in H$, we have $ab = a(b^{-1})^{-1} \in H$, so H is closed under the operation.

2.7 Theorem: (*The Finite Subgroup Test*) *Let G be a group and let H be a finite subset of H. Then $H \leq G$ if and only if*

(1) $H \neq \emptyset$, and
(2) H is closed under the operation, that is $ab \in H$ for all $a, b \in H$.

Proof: The proof is left as an exercise.

2.8 Example: The set $\big\{(x, y) \in \mathbb{R}^2 \big| xy \geq 0\big\}$ is not a subgroup of $\mathbb{R}^2$ since it is not closed under addition.

2.9 Example: For $n \in \mathbb{Z}^+$ we have $C_n \leq C_\infty \leq \mathrm{S}^1 \leq \mathbb{C}^*$ where

$$\begin{aligned} C_n &= \big\{z \in \mathbb{C}^* \big| z^n = 1\big\} \\ C_\infty &= \big\{z \in \mathbb{C}^* \big| z^n = 1 \text{ for some } n \in \mathbb{Z}^+\big\} \\ \mathrm{S}^1 &= \big\{z \in \mathbb{C}^* \big| \|z\| = 1\big\} \end{aligned}$$

2.10 Example: Given a commutative ring R, in the general linear group $GL_n(R)$ we have the following subgroups, called the **special linear group**, the **orthogonal group** and the **special orthogonal group**.

$$\begin{aligned} SL_n(R) &= \big\{A \in M_n(R) \big| \det(A) = 1\big\} \\ O_n(R) &= \big\{A \in M_n(R) \big| A^TA = I\big\} \\ SO_n(R) &= \big\{A \in M_n(R) \big| A^TA = I, \det(A) = 1\big\} \end{aligned}$$

2.11 Example: For $\theta \in \mathbb{R}$, the **rotation** in $\mathbb{R}^2$ about $(0,0)$ by the angle θ is given by the matrix

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

and the **reflection** in $\mathbb{R}^2$ in the line through $(0,0)$ and the point $\left(\cos\frac{\theta}{2}, \sin\frac{\theta}{2}\right)$ is given by the matrix

$$F_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

We have

$$\begin{aligned} O_2(\mathbb{R}) &= \big\{R_\theta, F_\theta \big| \theta \in \mathbb{R}\big\} \\ SO_2(\mathbb{R}) &= \big\{R_\theta \big| \theta \in \mathbb{R}\big\} \end{aligned}$$

In $O_2(\mathbb{R})$, for $\alpha, \beta \in \mathbb{R}$ we have

$$F_\beta F_\alpha = R_{\beta-\alpha} \;,\; F_\beta R_\alpha = F_{\beta-\alpha} \;,\; R_\beta F_\alpha = F_{\alpha+\beta} \;,\; R_\beta R_\alpha = R_{\alpha+\beta}\,.$$

2.12 Example: For $n \in \mathbb{Z}^+$, the **dihedral group** D_n is the group

$$D_n = \big\{R_k, F_k \big| k \in \mathbb{Z}_n\big\} = \big\{R_0, R_1, \cdots, R_{n-1}, F_0, F_1, \cdots F_{n-1}\big\}$$

where for $k \in \mathbb{Z}_n$ we write $R_k = R_{\theta_k}$ and $F_k = F_{\theta_k}$ with $\theta_k = \frac{2\pi k}{n}$. We have

$$D_n \leq O_2(\mathbb{R}) \leq GL_2(\mathbb{R}) \leq \mathrm{Perm}(\mathbb{R}^2)$$

and for $k, l \in \mathbb{Z}_n$, the operation in D_n is given by

$$F_l F_k = F_{l-k} \;,\; F_l R_k = F_{l-k} \;,\; R_l F_k = F_{k+l} \;,\; R_l R_k = R_{k+l}\,.$$

2.13 Definition: Let G be a group and let $a \in G$. The **centre** of G is the set

$$Z(G) = \big\{a \in G \big| ax = xa \text{ for all } x \in G\big\}$$

and the **centralizer** of a in G to be the set

$$C(a) = C_G(a) = \big\{x \in G \big| ax = xa\big\}\,.$$

As an exercise, show that $Z(G)$ and $C_G(a)$ are both subgroups of G.

2.14 Example: Find the centre of D_4 and find the centralizers of R_k and F_k in D_4.

2.15 Example: If H and K are subgroups of G then so is $H \cap K$. More generally, if A is a set and $H_\alpha \leq G$ for each $\alpha \in A$, then $\bigcap_{\alpha \in A} H_\alpha \leq G$ by the Subgroup Test II. Indeed we have $e_G \in H_\alpha$ for all $\alpha \in A$ so that $e_G \in \bigcap_{\alpha \in A} H_\alpha$, and if $a, b \in \bigcap_{\alpha \in A} H_\alpha$ then for every $\alpha \in A$ we have $a, b \in H_\alpha$ hence $ab^{-1} \in H_\alpha$, and so $ab^{-1} \in \bigcap_{\alpha \in A} H_\alpha$.

2.16 Definition: Let G be a group and let $S \subseteq G$. The **subgroup of** G **generated by** S, denoted by $\langle S \rangle$, is the smallest subgroup of G which contains S, that is the intersection of all subgroups of G which contain S. The elements of S are called **generators** of the group $\langle S \rangle$. When S is a finite set, we omit set brackets and write $\langle a_1, a_2, \cdots, a_n \rangle = \big\langle \{a_1, a_2, \cdots, a_n\} \big\rangle$. A **cyclic subgroup** of G is a subgroup of the form $\langle a \rangle$ for some $a \in G$. For $a \in G$, the subgroup $\langle a \rangle$ is called the **cyclic subgroup of** G **generated by** a. When $G = \langle a \rangle$ for some $a \in G$ we say that G is **cyclic**.

2.17 Theorem: (*Elements of a Cyclic Group*) *Let G be a group and let $a \in G$. Then*
(1) we have $\langle a \rangle = \big\{ a^k \big| k \in \mathbb{Z} \big\}$.
(2) If $|a| = \infty$ then the elements a^k with $k \in \mathbb{Z}$ are all distinct so we have $\big|\langle a \rangle\big| = \infty$.
(3) If $|a| = n$ then for $k, \ell \in \mathbb{Z}$ we have $a^k = a^\ell \iff k = \ell \bmod n$ and so

$$\langle a \rangle = \big\{ a^k \big| k \in \mathbb{Z}^n \big\} = \big\{ e, a, a^2, \cdots, a^{n-1} \big\}$$

with the listed elements all distinct so that $\big|\langle a \rangle\big| = n$. In particular, $a^k = e \iff n \big| k$.

Proof: First we show that $\langle a \rangle = \big\{ a^k \big| k \in \mathbb{Z} \big\}$. By definition, $\langle a \rangle$ is the intersection of all subgroups $H \leq G$ with $a \in H$. By closure under the operation and under inversion, if $H \leq G$ with $a \in H$ then $a^k \in H$ for all $k \in \mathbb{Z}$, and so $\big\{ a^k \big| k \in \mathbb{Z} \big\} \subseteq \langle a \rangle$. On the other hand, since $e = a^0$, $a^k (a^l)^{-1} = a^{k-l}$, we see that $\big\{ a^k \big| k \in \mathbb{Z} \big\}$ is a subgroup of G (by the Subgroup Test) and we have $a = a^1 \in \big\{ a^k \big| k \in \mathbb{Z} \big\}$, and so $\langle a \rangle \subseteq \big\{ a^k \big| k \in \mathbb{Z} \big\}$.

Now suppose that $|a| = \infty$ and suppose, for a contradiction, that $a^k = a^\ell$ with $k < \ell$. Then $a^{\ell - k} = a^\ell (a^k)^{-1} = a^\ell (a^\ell)^{-1} = e$ but this contradicts the fact that $|a| = \infty$.

Next suppose that $|a| = n$. Suppose that $a^k = a^\ell$. Then, as above, $a^{\ell - k} = e$. Write $\ell - k = qn + r$ with $0 \leq r < n$. Then $e = a^{\ell - k} = a^{qn + r} = (a^n)^q a^r = a^r$. Since $|a| = n$ we must have $r = 0$. Thus $\ell - k = qn$, that is $k = \ell \bmod n$. Conversely, suppose that $k = \ell \bmod n$, say $k = \ell + qn$. Then $a^k = a^{\ell + qn} = a^\ell (a^n)^q = a^\ell$.

2.18 Notation: When G is an abelian group under $+$, we have $\langle a \rangle = \{ka | k \in \mathbb{Z}\}$.

2.19 Example: The groups $\mathbb{Z}$ and $\mathbb{Z}_n$ are cyclic with $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}_n = \langle 1 \rangle$. The group $C_n = \{z \in \mathbb{C}^* | z^n = 1\}$ is cyclic with $C_n = \big\langle e^{i\, 2\pi/n} \big\rangle$.

2.20 Example: In the group $\mathbb{Z}$ we have $\langle 2 \rangle = \{\cdots, -2, 0, 2, 4, \cdots\}$, but in the group $\mathbb{R}^*$ we have $\langle 2 \rangle = \big\{ \cdots \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \cdots \big\}$.

2.21 Example: The group $U_{18} = \{1, 5, 7, 11, 13, 17\}$ is cyclic with $U_{18} = \langle 5 \rangle$ because in U_{18} we have

k	0	1	2	3	4	5
5^k	1	5	7	17	13	11

2.22 Example: If G and H are groups then $\big|G\times H\big|=|G|\,|H|$. For $a\in G$ and $b\in H$,

$$\big|(a,b)\big| = \operatorname{lcm}\big(|a|,|b|\big)\,.$$

Indeed if $|a|=n$ and $|b|=m$ then for $k\in\mathbb{Z}$ we have

$$\begin{aligned}(a,b)^k=e_{G\times H} &\iff (a^k,b^k)=(e_G,e_H)\\ &\iff \big(a^k=e_G \text{ and } b^k=e_H\big)\\ &\iff n\big|k \text{ and } m\big|k\big)\\ &\iff\ k \text{ is a common multiple of } n \text{ and } m.\end{aligned}$$

2.23 Theorem: (*The Classification of Subgroups of a Cyclic Group*) *Let G be group and let $a\in G$.*

(1) Every subgroup of $\langle a\rangle$ is cyclic.

(2) If $|a|=\infty$ then $\langle a^k\rangle=\langle a^\ell\rangle \iff \ell=\pm k$ so the distinct subgroups of $\langle a\rangle$ are the trivial group $\langle a^0\rangle=\{e\}$ and the groups $\langle a^d\rangle=\big\{a^{kd}\big|k\in\mathbb{Z}\big\}$ with $d\in\mathbb{Z}^+$.

(3) If $|a|=n$ then we have $\langle a^k\rangle=\langle a^\ell\rangle \iff \gcd(k,n)=\gcd(\ell,n)$ and so the distinct subgroups of $\langle a\rangle$ are the groups $\langle a^d\rangle=\big\{a^{kd}\big|k\in\mathbb{Z}_{n/d}\big\}=\big\{a^0,a^d,a^{2d},\cdots,a^{n-d}\big\}$ where d is a positive divisor of n.

Proof: First we show that every subgroup of $\langle a\rangle$ is cyclic. Let $H\le\langle a\rangle$. If $H=\{e\}$ then $H=\langle e\rangle$, which is cyclic. Suppose that $H\ne\{e\}$. Note that H contains some element of the form a^k with $k\in\mathbb{Z}^+$ since we can choose $a^\ell\in H$ for some $\ell\ne0$, and if $\ell<0$ then we also have $a^{-\ell}=(a^\ell)^{-1}\in H$. Let k be the smallest positive integer such that $a^k\in H$. We claim that $H=\langle a^k\rangle$. Since $a^k\in H$, by closure under the operation and under inversion we have $(a^k)^j\in H$ for all $j\in\mathbb{Z}$ and so $\langle a^k\rangle\subseteq H$. Let $a^\ell\in H$, where $\ell\in\mathbb{Z}$. Write $\ell=kq+r$ with $0\le r<k$. Then $a^\ell=a^{kq}a^r$ so we have $a^r=a^\ell(a^{kq})^{-1}\in H$. By our choice of k we must have $r=0$, so $\ell=qk$ and so $a^\ell\in\langle a^k\rangle$. Thus $H\subseteq\langle a^k\rangle$.

Suppose that $|a|=\infty$. If $\ell=\pm k$ then clearly $\langle a^\ell\rangle=\langle a^k\rangle$. Suppose that $\langle a^\ell\rangle=\langle a^k\rangle$. Since $a^k\in\langle a^\ell\rangle$ we have $k=\ell t$ for some $t\in\mathbb{Z}$, so $\ell\big|k$. Similarly, since $a^\ell\in\langle a^k\rangle$ we have $k\big|\ell$. Since $k\big|\ell$ and $\ell\big|k$ we have $\ell=\pm k$.

Now suppose that $|a|=n$. Note first that for any divisor $d\big|n$ we have

$$\langle a^d\rangle=\big\{a^{dk}\big|k\in\mathbb{Z}_{n/d}\big\}=\big\{a^0,a^d,a^{2d},\cdots,a^{n-d}\big\}$$

with the listed elements distinct so that $|a^d|=\frac{n}{d}$. We claim that $\langle a^k\rangle=\langle a^d\rangle$ where $d=\gcd(k,n)$. Since $d\big|k$ we have $a^k\in\langle a^d\rangle$ so $\langle a^k\rangle\subseteq\langle a^d\rangle$. Choose $s,t\in\mathbb{Z}$ so that $ks+nt=d$. Then $a^d=a^{ks+nt}=(a^k)^s(a^n)^t=(a^k)^s\in\langle a^k\rangle$ and so $\langle a^d\rangle\subseteq\langle a^k\rangle$. Thus $\langle a^k\rangle=\langle a^d\rangle$, as claimed. Now if $\langle a^k\rangle=\langle a^\ell\rangle$ and $d=\gcd(k,n)$ and $c=\gcd(\ell,n)$ then $\langle a^d\rangle=\langle a^k\rangle=\langle a^\ell\rangle=\langle a^c\rangle$ and so $\big|\langle a^d\rangle\big|=\big|\langle a^c\rangle\big|$, that is $\frac{n}{d}=\frac{n}{c}$, and so $d=c$. Conversely, if $d=\gcd(k,n)=\gcd(\ell,n)=c$ then we have $\langle a^k\rangle=\langle a^d\rangle=\langle a^\ell\rangle$.

2.24 Corollary: (*Orders of Elements in a Cyclic Group*) *Let G be a group and let $a\in G$.*
(1) If $|a|=\infty$ then $|a^0|=1$ and $a^k=\infty$ for $k\ne0$, and
(2) if $|a|=n$ then $|a^k|=\frac{n}{\gcd(k,n)}$.

2.25 Corollary: (*Generators of a Cyclic Group*) *Let G be a group and let $a\in G$. Then*
(1) if $|a|=\infty$ then $\langle a^k\rangle=\langle a\rangle \iff k=\pm1$, and
(2) if $|a|=n$ then $\langle a^k\rangle=\langle a\rangle \iff \gcd(k,n)=1 \iff k\in U_n$.

2.26 Corollary: (*The Number of Elements of Each Order in a Cyclic Group*) *Let G be a group and let $a \in G$ with $|a| = n$. Then for each $k \in \mathbb{Z}$, the order of a^k is a positive divisor of n, and for each positive divisor $d\big|n$, the number of elements in $\langle a\rangle$ of order d is equal to $\varphi(d)$.*

2.27 Corollary: F*or $n \in \mathbb{Z}^+$ we have $\sum\limits_{d|n} \varphi(d) = n$.*

2.28 Corollary: (*The Number of Elements of Each Order in a Finite Group*) *Let G be a finite group. For each $d \in \mathbb{Z}^+$, the number of elements in G of order d is equal to $\varphi(d)$ multiplied by the number of cyclic subgroups of G of order d.*

2.29 Theorem: (*Elements of $\langle S\rangle$*) *Let G be a group and let $\emptyset \neq S \subseteq G$. Then*

$$\begin{aligned}\langle S\rangle &= \left\{{a_1}^{k_1}{a_2}^{k_2}\cdots{a_\ell}^{k_\ell}\big|\ell \geq 0, a_i \in S, k_i \in \mathbb{Z}\right\}\\ &= \left\{{a_1}^{k_1}{a_2}^{k_2}\cdots{a_\ell}^{k_\ell}\big|\ell \geq 0, a_i \in S \text{ with } a_i \neq a_{i+1}, 0 \neq k_i \in \mathbb{Z}\right\}\end{aligned}$$

where the empty product (when $\ell = 0$) is the identity element. If G is abelian then

$$\langle S\rangle = \left\{{a_1}^{k_1}{a_2}^{k_2}\cdots{a_\ell}^{k_\ell}\big|\ell \geq 0, a_i \in S \text{ with } a_i \neq a_j \text{ for } i \neq j, 0 \neq k_i \in \mathbb{Z}\right\}.$$

Proof: The proof is left as an exercise.

2.30 Notation: If G is an abelian group under $+$ then

$$\langle S\rangle = \text{Span}_\mathbb{Z}\{S\} = \left\{k_1a_1 + k_2a_2 + \cdots + k_\ell a_\ell\big|\ell \geq 0, a_i \in S \text{ with } a_i \neq a_j, 0 \neq k_i \in \mathbb{Z}\right\}.$$

2.31 Example: As an exercise, show that in $\mathbb{Z}$ we have $\langle k, \ell\rangle = \langle d\rangle$ where $d = \gcd(k, \ell)$.

2.32 Example: In $\mathbb{Z}^2$, the elements of $\big\langle(1, 3), (2, 1)\big\rangle$ are the vertices of parallelograms which cover $\mathbb{R}^2$.

2.33 Example: We have $D_n = \big\langle R_1, F_0\big\rangle$ in $O_2(\mathbb{R})$ because $R_k = {R_1}^k$ and $F_k = R_kF_0$.

2.34 Definition: Let S be a set. The **free group** on S is the set whose elements are

$$F(S) = \left\{{a_1}^{k_1}{a_2}^{k_2}\cdots{a_\ell}^{k_\ell}\big|\ell \geq 0, a_i \in S, 0 \neq k_i \in \mathbb{Z}\right\}$$

with the operation given by concatenation

$$({a_1}^{j_1}\cdots{a_\ell}^{j_\ell})({b_1}^{k_1}\cdots{b_m}^{k_m}) = {a_1}^{j_1}\cdots{a_\ell}^{j_\ell}{b_1}^{k_1}\cdots{b_m}^{k_m}$$

followed by grouping and cancellation in the sense that if $a_\ell = b_1$ then we replace ${a_\ell}^{j_\ell}{b_1}^{k_1}$ by ${a_\ell}^{j_\ell+k_1}$ and if, in addition, $j_\ell + k_1 = 0$ then we omit the term ${a_\ell}^0$ and perform further grouping if $a_{\ell-1} = b_2$. For example, in $F(a, b)$ we have

$$(a\,b^2a^{-3}b)(b^{-1}a^3b\,a^{-2}) = a\,b^2a^{-3}b\,b^{-1}a^3b\,a^{-2} = a\,b^2a^{-3}a^3b\,a^{-2} = a\,b^2b\,a^{-2} = a\,b^3a^{-2}.$$

Note that in the free group $F(S)$ we have $F(S) = \langle S\rangle$.

2.35 Definition: Let S be a set. The **free abelian group** on S is the set

$$A(S) = \left\{k_1a_1 + \cdots + k_\ell a_\ell\big|\ell \geq 0, a_i \in S \text{ with } a_i \neq a_j, 0 \neq k_i \in \mathbb{Z}\right\}.$$

If we identify the element $k_1a_1 + k_2a_2 + \cdots + k_\ell a_\ell$ with the function $f : S \to \mathbb{Z}$ given by $f(a_i) = k_i$ and $f(a) = 0$ for $a \neq a_i$ for any i, then we can identify $A(S)$ with the set

$$A(S) = \sum_{a\in S}\mathbb{Z} = \left\{f : S \to \mathbb{Z}\big|f(a) = 0 \text{ for all but finitely many } a \in S\right\}.$$

Under this identification, we use the operation given by $(f + g)(a) = f(a) + g(a)$.