Definition 13.1

Let G be a group and $H \subseteq G$ a subgroup. For $a \in G$ the *left coset of H in G containing a* is the subset of G given by

$$aH = \{ah \mid h \in H\}$$

Similarly, the *right coset of H in G containing a* is the subset

$$Ha = \{ha \mid h \in H\}$$

Example. Consider the group D_4:

$\circ$	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
I	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	I	D'	D	H	V
R_{180}	R_{180}	R_{270}	I	R_{90}	V	H	D'	D
R_{270}	R_{270}	I	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	I	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	I	R_{270}	R_{90}
D	D	H	D'	V	R_{270}	R_{90}	I	R_{180}
D'	D'	V	D	H	R_{90}	R_{270}	R_{180}	I

Take the subgroup $K = \{I, H\}$ of D_4. Here are some left and right cosets of K in D_4:

$$\begin{array}{ll} R_{90}K = \{R_{90}, D'\} & KR_{90} = \{R_{90}, D\} \\ D'K = \{D', R_{90}\} & KD' = \{D', R_{270}\} \\ DK = \{D, R_{270}\} & KD = \{D, R_{90}\} \end{array}$$

Notice that:

- Cosets defined by different elements may be the same. E.g. $R_{90}K = D'K$.
- Left coset of a given element may be different that the right coset. For example, $R_{90}K \neq KR_{90}$.

Theorem 13.2

Let G be a group, $H \subseteq G$ a subgroup, and let $a, b \in G$. Then:

1) $a \in aH$.
2) either $aH = bH$ or $aH \cap bH = \varnothing$.
3) $aH = bH$ if and only if $a^{-1}b \in H$.
4) $|aH| = |H|$, where $|aH|$ denotes the number of elements in aH.

Analogous properties hold for right cosets.

Proof.

1) Since $e \in H$ thus $a = ae \in aH$.

2) Assume that $aH \cap bH \neq \varnothing$ and let $g \in aH \cap bH$. Then $ah_1 = g = bh_2$ Then for $h \in H$ we have

$$ah = ah_1(h_1^{-1}h) = bh_2(h_1^{-1}h) \in bH$$

This shows that $aH \subseteq bH$. By a similar argument $bH \subseteq aH$, so $aH = bH$.

3) If $aH = bH$ then $b = ah$ for some $h \in H$, so $a^{-1}b = h \in H$. Conversely, if $a^{-1}b = h \in H$ then $b \in aH \cap bH$. By part 2) this gives $aH = bH$.

4) It is enough to notice that the function $f\colon H \to aH$, $f(h) = ah$ is a bijection. $\square$

Definition 13.3

For a group G and a subgroup $H \subseteq G$ by G/H we denote the set of left cosets of H in G and by $H\backslash G$ we denote the set of right cosets.

Example. Cosets of $K = \{I, H\}$ in D_4:

I	H
R_{90}	D'
R_{180}	V
R_{270}	D

G/H
left cosets

I	H
R_{90}	D
R_{180}	V
R_{270}	D'

$H\backslash G$
right cosets

Theorem 13.4

If G is a group and $H \subseteq G$ is a subgroup, then $|G/H| = |H\backslash G|$.

Proof. The function $f\colon G/H \to H\backslash G$ given by $f(aH) = Ha^{-1}$ is a bijection. □

Definition 13.5

If G is a group and $H \subseteq G$ is a subgroup then the *index* of H, denoted $[G : H]$, is the number of left cosets of H in G (or, equivalently, the number of right cosets):

$$[G : H] = |G/H| = |H\backslash G|$$

Example. If $K = \{I, H\} \subseteq D_4$ then $[D_4 : K] = 4$.

Theorem 13.6 (Lagrange Theorem)

If G is a finite group and $H \subseteq G$ is a subgroup then

$$|G| = [G : H] \cdot |H|$$

Proof. By Theorem 13.2 each element of G belongs to exactly one left coset of H. Thus, if $a_1H,\ a_2H, \dots, a_nH$ are all distinct cosets, then

$$|G| = |a_1H| + |a_2H| + \ldots + |a_nH|$$

Moreover, since each coset consists of $|H|$ elements and there are $[G\colon H]$ cosets, we obtain that $|G| = [G : H] \cdot |H|$. □

Corollary 13.7

If G is a finite group and $H \subseteq G$ is a subgroup then the order of H divides the order of G.

Corollary 13.8

If G is a finite group and $a \in G$ then the order $|a|$ of a divides the order of G.

Proof. Recall that by Theorem 7.8 we have $|a| = |\langle a \rangle|$ where $\langle a \rangle$ is the subgroup of G generated by a. Also, by Corollary 13.7, $|\langle a \rangle|$ divides $|G|$.

□

Note. It is not true that if G is a group and k divides $|G|$ then G contains an element of order k. Take for example the symmetric group S_4. By looking at possible disjoint cycle decompositions of elements of S_4, we can see that every element of S_4 has order 1,2,3 or 4. This means that S_4 does not contain any element of order 6, even though 6 divides the order of S_4.

Note. It is also not true that if k divides the order of a group G, then G contains a subgroup H of order k. We will see an example of that later.

Example. Let G be a group of order p where p is a prime number. Then every element of G is of order either 1 (i.e. it is the identity element) or p. Thus if $a \in G$ and $a \neq e$ then $|a| = |G|$. This means that G is a cyclic group generated by a, and so $G \cong \mathbb{Z}_p$.

Example. We will show if G is a group of order 4, then G is isomorphic either to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. By Corollary 13.8, if $a \in G$ then $|a| = 1$ (which means that $a = e$), $|a| = 2$, or $|a| = 4$. If G contrains an element of order 4, then it is cyclic, and so $G \cong \mathbb{Z}_4$. Otherwise, G contains the trivial element e and three elements, (which we will denote a, b, c) of order 2. Notice that $ab = ba = c$ (since $ab = b$ would give $a = e$, $ab = a$ would give $b = e$, and $ab = e = aa$ would imply that $b = a$). Similarly, we obtain that $ac = ca = b$ and $bc = bc = a$. This shows that the function $f\colon G \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$, given by $f(a) = (1, 0)$, $f(b) = (0, 1)$ and $f(c) = (1, 1)$ is an isomorphism of groups.