7 Cosets and Lagrange's Theorem

Definition. Let G be a group and H its subgroup. We define

the left coset of H containing a: $aH = \{ah \mid h \in H\}$
the right coset of H containing a: $Ha = \{ha \mid h \in H\}$

The element a is called a *coset representative* of aH or Ha.

Example. Consider the subgroup $4\mathbf{Z}$ of $\mathbf{Z}$. List the left cosets (same as right) of this subgroup.

Example. Consider the subgroup $H = \{\alpha \in S_5 \mid \alpha(1) = 1\}$ of S_5. List the left and the right cosets of this subgroup and show that they are not equal. Furthermore, show there is an $\alpha \in G$ such that $\alpha H \alpha^{-1} \neq H$.

Note. In our examples, the cosets were either disjoint or equal. Only one of the cosets is a subgroup — the one containing the identity.

Lemma. Let H be a subgroup of G and let $a, b \in G$. Then the following hold for left cosets, and analogous statements are true for right cosets.

1) $a \in aH$
2) $aH = H$ if and only if $a \in H$
3) $(ab)H = a(bH)$
4) $aH = bH$ if and only if $a \in bH$.
5) $aH = bH$ or $aH \cap bH = \emptyset$.
6) $aH = bH$ if and only if $a^{-1}b \in H$ and $Ha = Hb$ if and only if $ba^{-1} \in H$.
7) $|aH| = |bH| = |H|$
8) $aH = Ha$ if and only if $aHa^{-1} = H$
9) aH is a subgroup of G if and only if $a \in H$, so $aH = H$.

Proof.

Note. The bijection $x \mapsto x^{-1}$ sends every coset aH to Ha^{-1}, establishing a bijective correspondence between the collections of left and right cosets.

Lagrange's Theorem 7.1. If G is a finite group and H a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left or right cosets of H in G is $|G|/|H|$.

Proof.

Definition. The *index of a subgroup H in G* is the number of left (or right) cosets of H in G. It is denoted by $|G : H|$.

Note. G and H need not be finite subgroups for the index to be defined, for example $|\mathbf{Z} : 4\mathbf{Z}| = 4$.

Corollaries to Theorem 7.1. Let H be a subgroup of G and let $a \in G$. Then

1) If G is finite, then $|G : H| = \dfrac{|G|}{|H|}$
2) If G is finite and $a \in G$, the order of a divides the order of G.
3) Every group of prime order is cyclic, hence isomorphic to $\mathbf{Z}_p$ for some prime p.
4) $a^{|G|} = e$
5) **Fermat's Little Theorem:** For every integer a and every prime p,
   $a^p \bmod p = a \bmod p$.

Proof.

Example. Inspired by Lagrange's theorem, one could ask: if k divides $|G|$, must there exist a subgroup of order k in G? This is true for cyclic groups, but not in general. Show that A_4 does not have a subgroup of order 6, yet $|A_4| = 12$ and $6|12$.

Theorem 7.2. Let H and K be two finite subgroups of a group, and consider the set $HK = \{hk \mid h \in H, k \in K\}$ (may not be a subgroup). Then $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

Proof.

Theorem 7.3. Every group of order $2p$, where p is prime, is isomorphic to either Z_{2p} or D_p.

Proof.

8 Direct Product

Definition. The *direct product* of groups $G_1, \dots, G_n$ is the set $G_1 \times \cdots \times G_n$ of n-tuples for which the i-th component is in G_i and the componentwise operation

$$(g_1, \dots, g_n)(g_1', \dots, g_n') = (g_1 g_n', \dots, g_n g_n')$$

Note. The textbook uses $\oplus$ instead of $\times$, but $\oplus$ is usually used when all groups $G_1, \dots, G_n$ are abelian.

Example. The group $\mathbf{Z} \times \mathbf{Z}$ is all pairs (x, y) where both coordinates are integers, may be imagined as the set of all vectors in the plane with initial point the origin and the terminal a point whose both coordinages are integers.

Example. The group $\mathbf{Z}_3 \times \mathbf{Z}_4$ has 12 elements. What is the order of the element $(1, 3)$?

Example. Every group of order 4 is isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Theorem 8.1. For an element $(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n)$, where every G_i, $i = 1, \ldots, n$ is finite, we have

$$|(g_1, \ldots, g_n)| = \mathrm{lcm}(|g_1|, \ldots, |g_n|)$$

Proof.

Example. Show that $\mathbf{Z}_8 \times \mathbf{Z}_{15}$ is cyclic of order 120, thus isomorphic to $\mathbf{Z}_{120}$.

Theorem 8.2. Let G and H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

Proof.

Corollary. Let $G_1, \ldots, G_n$ be finite cyclic groups.

1) $G_1 \times \cdots \times G_n$ is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.
2) $\mathbf{Z}_{n_1 \ldots n_k} \approx \mathbf{Z}_{n_1} \times \cdots \times \mathbf{Z}_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

Direct products help us better understand groups by breaking them up into smaller groups. For example, we can use it on the groups $U(n)$.

Definition. If k divides n, we define

$$U_k(n) = \{x \in U(n) \mid x \bmod k = 1\} = \{1 + kq \mid 1 + kq \in U(n)\}$$

It is not hard to see that $U_k(n)$ is a subgroup of $U(n)$.

Example. For every divisor k of 20, determine $U_k(20)$.

Theorem 8.3. Let s and t be relatively prime. Then

$$U_s(st) \approx U(t) \qquad U_t(st) \approx U(s) \qquad U(st) \approx U(s) \times U(t)$$

Corollary. If $n = n_1 n_2 \dots n_k$, and $\gcd(n_i, n_j) = 1$ when $i \neq j$, then

$$U(n) = U(n_1) \times U(n_2) \times \cdots \times U(n_k)$$

Note. Due to prime factorization, this means we only need to know what $U(p^n)$ is for a prime p:

$$U(2) = \{0\} \qquad U(2^n) = \mathbf{Z}_2 \times \mathbf{Z}_{2^{n-2}}, \text{ for } n \geq 2 \qquad U(p^n) = \mathbf{Z}_{p^n - p^{n-1}}, \text{ for } p \text{ prime } n \geq 1$$

Example. Determine $U(42)$ and $U(36)$.

Note. It is now a lot easier to see what orders of elements $U(n)$ has.

Proposition. Let $H, G_1, \ldots, G_n$ be groups. Then

1) The map $i_k : G_k \to G_1 \times \cdots \times G_n$ given by $i_k(g_k) = (e_1, \ldots, e_{k-1}, g_k, e_{k+1}, \ldots, e_n)$ is an isomorphism onto a subgroup of $G_1 \times \cdots \times G_n$, called *the inclusion of the k-th component*. Thus, we may think of G_k as a subgroup of $G_1 \times \cdots \times G_n$.
2) The map $p_k : G_1 \times \cdots \times G_n \to G_k$ given by $p_k(g_1, \ldots, g_n) = g_k$ is a homomorphism onto G_k, called *the projection to the k-th component.*
3) A map $f : H \to G_1 \times \cdots \times G_n$ is a homomorphism if and only if $p_k f : H \to G_k$ is a homomorphism. In that case $f(h) = (p_1 f(h), \ldots, p_n f(h))$.

Proof: easy!

Proof of Theorem 8.3. Also, follow the proof on the example of $U(20)$.