Section 44. Algebra and Groups

Note. In this section we give a quick introduction to groups, subgroups, and cosets. We will see later that mappings of $\mathbb{C}$ for groups.

Definition. Let G be a set of elements and $*$ a binary operation on G (that is, $* : G \times G \to G$). This is a *group* if the following hold:

The Associative Law. $p * (q * r) = (p * q) * r$ for all $p, q, r \in G$.

The Identity Law. $p * i = i * p = p$ for all $p \in G$ and some some $i \in G$. i is called the *identity* of G.

The Inverse Law. For any $p \in G$ there exists a $p' \in G$ such that $p * p' = p' * p = i$. Such p' is called an *inverse* of p, usually denoted p^{-1}.

Note. A detailed account of group theory can be in my online notes for Introduction to Modern Algebra (MATH 4127/5127) at:

`http://faculty.etsu.edu/gardnerr/4127/notes.htm`.

Note. It is straightforward to show that there is a unique identity in a group and that each $p \in G$ has a unique inverse (see page 18 of the book). We usually abbreviate the binary operation as $p * q = pq$. Notice that we do not assume that the binary operation is commutative.

Definition. A group G for which $pq = qp$ for all $p, q \in G$ is called an *Abelian group*.

Example. The real numbers under addition form an Abelian group. The set of all 2×2 invertible matrices with real entries form a non-Abelian group.

Definition. A *subgroup* of a given group G is a group whose elements lie in G and which has the same binary operation as G (Of course we require the subgroup to be closed under the binary operation.)

Example. We consider now some groups under addition. The rational $\mathbb{Q}$ are a subgroup of $\mathbb{R}$. The integers $\mathbb{A}$ are a subgroup of $\mathbb{Q}$. The even integers $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ is a subgroup of $\mathbb{Z}$. The set of all 2×2 matrices with real entries and determinant 1 form a subgroup of all 2×2 invertible real matrices.

Theorem 44.2. Conditions for a Subgroup.

A nonempty subset H of a group G is a subgroup of G if and only if for every $a, b \in H$ we have (i) $b^{-1}, ab \in H$, or (ii) $ab^{-1} \in H$.

Definition. Let G be a group with subgroup H. Let $a \in G$ be fixed. The set $\{ha \mid h \in H\}$ is a *right coset* of H (in G), denoted $\{ha\} = Ha$. A *left coset* of H in G is a set of the form $\{ah \mid h \in H\} = \{ah\} = aH$.

Example. Let $G = \mathbb{Z}$ and $H = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ a subgroup of G. Notice that G is an additive group so we use additive notation. The cosets of H are (since G is Abelian then the left and right cosets are the same):

$$0 + H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$1 + H = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

$$2 + H = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

This example suggests the following.

Theorem 44.4. The Identity of Cosets.
If Ha and Hb have one element in common then they coincide (that is, they are equal).

Corollary 44.4. Elements $a, b \in G$ lie in the same right coset of H if and only if $ab^{-1} \in H$.

Note 44.A. We can similarly show that $a, b \in G$ are in the same left coset of H if and only if $a^{-1}b \in H$.

Note 44.B. We see in the proof of Corollary 44.4 that the cosets of a subgroup of G partition G.

Example. Consider the additive group $G = \mathbb{C}$ and the additive subgroup $H = \mathbb{R}$. Geometrically, we represent $\mathbb{C}$ as the Gauss plane and $\mathbb{R}$ as the real axis of Gauss plane. For any $z \in \mathbb{C}$ with $z = a + ib$ (where $a, b \in \mathbb{R}$) we have the coset $H + z = \{h + (a + ib) \mid h \in H = \mathbb{R}\}$. Geometrically, this is the collection of points in $\mathbb{C}$ with imaginary parts equal to b. So the cosets partition the Gauss plane into uncountably many lines, each parallel to the real axis. Notice that z and z' are in the same coset if and only if they have the same imaginary parts; that is, if and only if $z - z' \in \mathbb{R} = H$, thus illustrating Corollary 44.4 for an additive group.

Theorem 44.5. Right and Left Cosets.
If the number of right cosets with respect to a subgroup H is finite, then there is an equal number of left cosets, and conversely.

Note. In the proof of Theorem 44.5, we demonstrated a one-to-one correspondence between the left cosets and the right cosets of a given subgroup. So the *cardinality* of the set of left cosets equals the cardinality of the set of right cosets. This does not depend on any *finiteness* of the collections of cosets.

Definition. Let G be a group and Ha a subgroup of G with a finite number of right cosets. The *index* of H in G is the number of right cosets (which is the same as the number of left cosets, by Theorem 44.5), denoted $[G : H]$. The *order* of a finite group G is the number of elements in the group, denoted $|G|$.

Note. Exercise 44.2 requires a proof of the following: "If H is a finite subgroup of a group G, then the number of distinct elements in any right coset Ha is always equal to the number of distinct elements in H. The same holds for any left coset aH.

Theorem 44.A. Lagrange's Theorem.
If G is a finite group and H is a subgroup of G then the order of H divides the order of G.

Revised: 3/1/2019