MATH500

Matthew Leonardson

Spring 2024

1 January 17, 2024

Definition 1.1. A *group* is a set G with a binary operation such that

1. $(xy)z = x(yz)$ for all $x, y, z \in G$.
2. There exists $e \in G$, the identity.
3. For all $x \in G$ there exists x^{-1} such that $xx^{-1} = e = x^{-1}x$.

Further, a group is *abelian* if

4. $xy = yx$ for all $x, y \in G$.

Definition 1.2. A *monoid* is a set M and a binary operation that only satisfy the first two axioms of 1.1.

Example 1.3. The following are examples of groups

- C_n: the cyclic group of order n. Written multiplicatively.
- $\mathbb{Z}/n$: the integers modulo n. Identical to C_n, but written additively.
- D_{2n}: the dihedral group[1] of order $2n$. Defined in 1.4.
- S_n: the symmetric group of degree n. All permuations of n numbers with the group operation being function composition.
- $GL_n(k)$: the general linear group of degree n. All invertible $n \times n$ matrices over a field k.
- Q_8: the quaternion group. Defined in 1.6.

[1] Some authors use D_n for the dihedral group of order $2n$.

Definition 1.4. The *dihedral group* of order $2n$ is the group of rotational symmetries of a regular n-gon in 3D space. More abstractly, it is a group with elements $\{r, s\}$ such that $r^n = s^2 = e$ and $rs = sr^{-1}$.

Remark 1.5. Bridging these two interpretations of the dihedral group, we can think of r as being a rotation of the n-gon and s as being a flipping of the n-gon.

Definition 1.6. The *quaternion group* is the set $\{\pm 1, \pm i, \pm j, \pm k\}$ and multiplication defined such that $(-1)^2 = 1$ and $i^2 = j^2 = k^2 = ijk = -1$.

Definition 1.7. Given a group G and subset H, we say H is a *subgroup* if

1. H is not empty.[2]
2. $x \in H$ implies $x^{-1} \in H$.
3. $x, y \in H$ implies $xy \in H$.

Definition 1.8. For a group G and $S \subseteq G$, the subgroup *generated* by S is

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

Fact 1.9. For a group G and $S \subseteq G$, $\langle S \rangle$ is a subgroup of G.

Definition 1.10. Given a group G and $S \subseteq G$, a *word* in S is $g \in G$ written $g = g_1 g_2 \dots g_n$ where $g_i \in S$ or $g_i^{-1} \in S$.

Fact 1.11. For a group G and $S \subseteq G$, the set of words in S is $\langle S \rangle$.

Definition 1.12. A group G is cyclic if there exists $a \in G$ such that $G = \langle a \rangle$.[3]

Fact 1.13. The order of $g \in G$ is equal to the cardinality of $\langle g \rangle$.

Definition 1.14. Given $H \leq G$, a *left coset* is $S \subseteq G$ where, for some $x \in G$, $S = xH = \{xh \mid h \in H\}$.

Definition 1.15. A *right* coset of G is $T \subseteq G$ such that $T = Hx$, for some $x \in G$.

Definition 1.16. G/H is the set of all left cosets of G, and $H \backslash G$ is the set of all right cosets of G.

Fact 1.17. All cosets have the same cardinality, meaning there is a bijection between any 2 cosets.

Fact 1.18. G/H and $H \backslash G$ have the same cardinality.

[2] This is equivalent to $e \in H$.

[3] This is abuse of notation, as we should write $\langle \{a\} \rangle$. However, this is rarely done.

Definition 1.19. The *index* of H in G is $|G/H|$ and written $|G : H|$.

Theorem 1.20 (Lagrange)**.** $H \leq G$ implies $|G| = |H| \cdot |G : H|$

Corollary 1.21. Given $K \leq H \leq G$, it holds that $|G : K| = |G : H| \cdot |H : K|$.

Definition 1.22. A *group homomorphism* is a function $\varphi : G \to H$ such that $\varphi(xy) = \varphi(x)\varphi(y)$.

Definition 1.23. For a field F, the *unit group* of F is $F^\times = F \setminus \{0\}$.

Definition 1.24. An *isomorphism* is a bijective homomorphism.

Definition 1.25. $N \leq G$ is *normal* if $xNx^{-1} = N$ for all $x \in G$.

Fact 1.26. For $\varphi : H \to G$ a group homomorphism, $\ker(\varphi)$ is a normal subgroup of H.

Definition 1.27. For N a normal subgroup of G, the *quotient group* G/N is N-cosets of G with multiplication defined by $xN \cdot yN = (xy)N$.