Abstract Algebra Notes

Cruz Godar

Math 481, 482, and 483/560
Professor Brussel
Cal Poly, Fall 2017–Spring 2018

I — Groups

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

1. $ab \in G$ for all $a, b \in G$.
2. $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. There is an $e \in G$ with $ae = ea = a$ for all $a \in G$.
4. For all $a \in G$, there is an $a^{-1} \in G$ with $aa^{-1} = a^{-1}a = e$.

Example: One important type of group is a *symmetry group*, formed by taking the collection S_X of symmetries of a set X — that is, structure-preserving bijections from X to itself. If $X = \mathbb{R}$, for instance, then S_X contains translational symmetries and stretching/shrinking ones.

Definition 1.2: Let $n \in \mathbb{N}$. The **integers modulo n** are the set $\mathbb{Z}_n = \{0, 1, ..., n-1\}$. $\mathbb{Z}_n$ is a group, with the operation given by addition mod n.

Definition 1.3: Let $n \in \mathbb{N}$. The group $\mathbf{U(n)}$ is defined as $U(n) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$, with the operation given by multiplication mod n.

Definition 1.4: The **dihedral group** of degree n is the the group D_n of symmetries of a regular n-gon, given by $D_n = \{e, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s\}$, where r is a rotation counter-clockwise by $\frac{2\pi}{n}$, s is a reflection over the x-axis, and the operation is function composition. Note that $sr = r^{-1}s$.

Definition 1.5: The **symmetric group** of degree n is the group S_n of permutations on n elements, defined as $\{\sigma : \{1, ..., n\} \twoheadrightarrow \{1, ..., n\}\}$, where each σ is a bijection and the operation is given by function composition. We use **cycle notation** to denote elements of S_n: the element $(124) \in S_4$, for example, denotes the function σ with $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(4) = 1$, and $\sigma(3) = 3$.

Definition 1.6: The **order** of a group G is $|G|$. A **finite group** is one that has finite order.

Definition 1.7: A group G is **Abelian** if $ab = ba$ for all $a, b \in G$.

Proposition 1.8: Let G be a group. Then $e \in G$ is unique.

Proof: Suppose there were $e, e' \in G$ such that $ae = ea = ae' = e'a = a$ for all $a \in G$. Then $ee' = e$ and $ee' = e'$, so $e = e'$.

Proposition 1.9: Let G be a group. If $ab = ac$ for $a, b, c \in G$, then $b = c$, and similarly, if $ab = cb$, then $a = c$.

Proposition 1.10: Let G be a group and $a \in G$. Then a^{-1} is unique.

Proof: If there were $a^{-1}, \left(a^{-1}\right)' \in G$ such that $aa^{-1} = a^{-1}a = a\left(a^{-1}\right)' = \left(a^{-1}\right)'a = e$, then $aa^{-1} = a\left(a^{-1}\right)'$, so $a^{-1}aa^{-1} = a^{-1}a\left(a^{-1}\right)'$, and so $a^{-1} = \left(a^{-1}\right)'$.

Definition 1.11: Let G be a group. A set $H \subseteq G$ is a **subgroup** of G, written $H \leq G$, if H is itself a group under G's operation.

Example: For all groups, the *trivial subgroup* $\{e\} \leq G$, and $G \leq G$.

Example: If X is a regular, nonoriented n-gon and X' is a regular, oriented n-gon (so reflections count as symmetries of X, but not of X'), then $S'_X \leq S_X$.

Example: $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is a group with its operation given by stretching and rotating the plane — $z = re^{i\theta}$ represents the symmetry of stretching by r and rotating by θ (or, equivalently, moving 1 to z). $S^1 = \{e^{i\theta} \mid \theta \in [0, 2\pi)\} = \{z \in \mathbb{C}^* \mid |z| = 1\}$ is also a group under the same operation, so $S^1 \leq C^*$.

Proposition 1.12: Let G be a group. Then $H \subseteq G$ is a subgroup of G if and only if

1. $H \neq \varnothing$.
2. $ab \in H$ for all $a, b \in H$.
3. For all $a \in H$, $a^{-1} \in H$.

Proof: ($\Rightarrow$) If $H \leq G$, then the only statement to prove is that the identity of H is the same as that of G, so that we can be sure that $a^{-1} \in H$ is the same as a^{-1} in G. If the two identities are e_G and e_H, then $e_H e_G = e_H$ in G and $e_H e_H = e_H$ in H, so $e_H e_G = e_H e_H$ in G, and therefore $e_G = e_H$. Thus the inverses are the same, and so all three conditions are met.

($\Leftarrow$) Let $a, b, c \in H$ (which is valid, since H is nonempty). Then $a, b, c \in G$, so $(ab)c = a(bc)$. Also, since $a^{-1} \in H$ (and this is the inverse from G), $aa^{-1} = e_G \in H$. We already know H is closed under G's operation, so $H \leq G$.

Definition 1.13: Let G be a group and $a \in G$. The **group generated by** $\boldsymbol{a}$ is $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Example: In D_n, $\langle r \rangle = \{e, r, r^2, ..., r^{n-1}\}$ and $\langle s \rangle = \{e, s\}$.

Definition 1.14: Let G be a group. The **order** of $a \in G$ is $|a| = |\langle a \rangle|$, or, equivalently, the smallest $n \in \mathbb{N}$ such that $a^n = e$ if it exists, or ∞ if it does not.

Definition 1.15: The orders of the elements in $U(9) = \{1, 2, 4, 5, 7, 8\}$ are

$$|1| = 1, \qquad |2| = 6, \qquad |4| = 3, \qquad |5| = 6, \qquad |7| = 3, \qquad |8| = 2.$$

Proposition 1.16: Let G be a group and $a \in G$. Then $|a| = \left|a^{-1}\right|$.

Proof: Since $a^k = e$ if and only if $\left(a^k\right)^{-1} = e$, if and only if $\left(a^{-1}\right)^k = e$, the smallest $n \in \mathbb{N}$ such that $a^n = e$ will also be the smallest $m \in \mathbb{N}$ such that $\left(a^{-1}\right)^m = e$. Thus $|a| = \left|a^{-1}\right|$.