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 **general linear group** of degree n over k is $GL_n(k) = \{A \in M_n(k) \mid \det A \neq 0\}$, with the operation given by matrix multiplication. Typically, k is $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}$.

Definition 1.7: The **special linear group** of degree n over k is $SL_n(k) = \{A \in M_n(k) \mid \det A = 1\}$, with the operation again given by matrix multiplication.

Definition 1.8: The **orthogonal group** of degree n is $O_n = \{A \in M_n(\mathbb{R}) \mid AA^{\mathrm{T}} = I\}$, and the **special orthogonal group** of degree n is $SO_n = \{A \in O_n \mid \det A = 1\}$. The **unitary group**, U_n, and **special unitary group**, SU_n, are defined identically, except their matrices are taken from $M_n(\mathbb{C})$ and require that $A\overline{A}^{\mathrm{T}} = I$.

Definition 1.9: The **order** of a group G is $|G|$. A **finite group** is one that has finite order.

Definition 1.10: A group G is **Abelian** if $ab = ba$ for all $a, b \in G$.

Proposition 1.11: 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 1.12: 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 1.13: 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 1.14: 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, $\{e\} \leq G$, called the *trivial subgroup*, 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 $S'_X \leq S_X$.

Definition 1.15: $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ 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 $S^1 \leq C^*$.

Definition 1.16: The **quaternions** are the set

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ijk = -1\}.$$

$\mathbb{H}$ forms a group under addition, and $\mathbb{H}^*$ a group under multiplication. Similarly to S^1, we define the **unit 3-sphere** as $S^3 = \{z \in \mathbb{H}^* \mid |z| = 1\} \leq \mathbb{H}^*$.

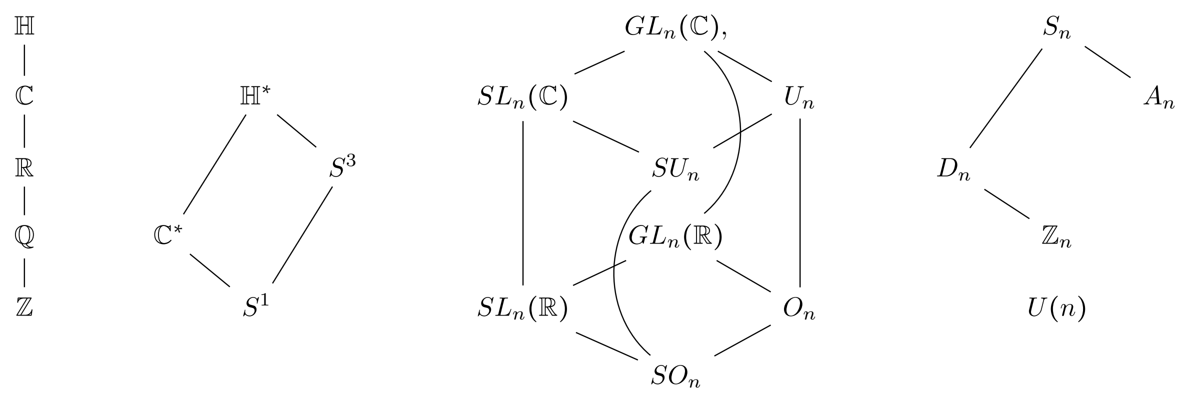
Proposition 1.17: Let G be a group. Then $H \subseteq G$ is a subgroup of G if and only if

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 $H \leq G$.

Example: The major groups:



Definition 1.18: Let G be a group and $a \in G$. The **group generated by 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 1.19: 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 1.20: The orders of the elements in $U(9) = \{1, 2, 4, 5, 7, 8\}$ are

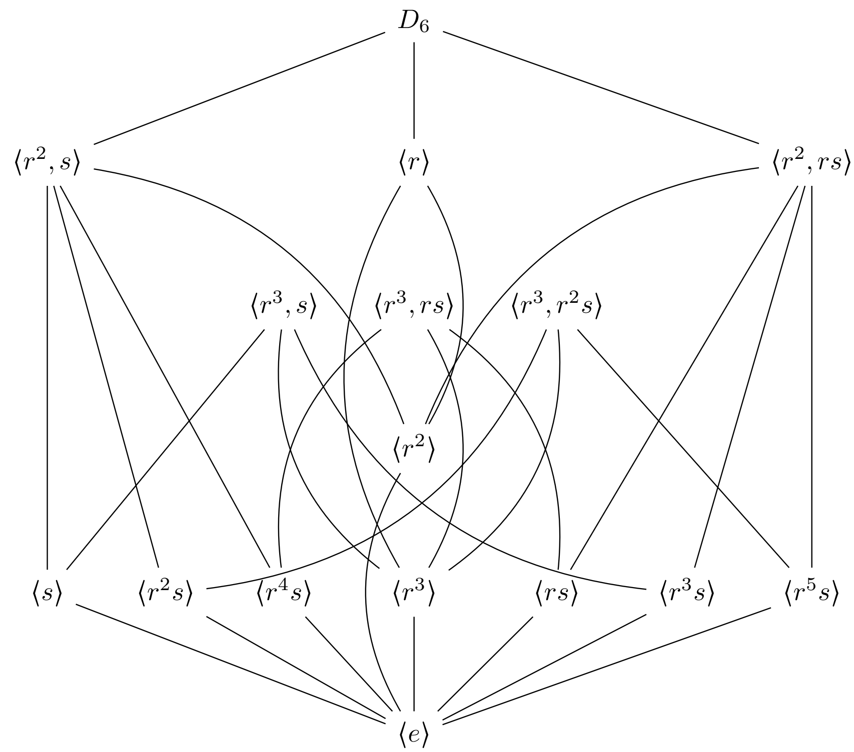
$$|1| = 1, \qquad |2| = 6, \qquad |4| = 3, \qquad |5| = 6, \qquad |7| = 3, \qquad |8| = 2.$$

Proposition 1.21: 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 $|a| = \left|a^{-1}\right|$.

Definition 1.22: A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$, called a **generator** of G.

Example: The subgroup lattice of D_6:

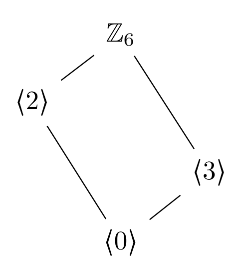


Theorem 1.23: A subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle a\rangle$ and $H \leq G$. Then for all $h \in H$, $h = a^m$ for some $m \in \mathbb{Z}$. Let $S = \{m \in \mathbb{N} \mid a^m \in H\}$, let m_0 be the minimum element of S, and let $h = a^m \in H$ be arbitrary. Then $m = m_0 q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < m_0$, so $a^m = a^{m_0 q + r}$, or equivalently, $a^r = a^{m - m_0 q}$. Since $a^m = h \in H$ and $a^{m_0 q} = (a^{m_0})^q \in H$, $a^{m - m_0 q} = a^r \in H$. Thus if $r \neq 0$, $r \in S$ by definition, but $r < m_0$, the smallest element in S. ↯ Thus $r = 0$, and so $h = (a^{m_0})^q$ for some $q \in \mathbb{Z}$. Since h was arbitrary, $H = \langle a^{m_0}\rangle$.

Example: Since $\mathbb{Z}$ is cyclic, every subgroup of $\mathbb{Z}$ is of the form $\langle a\rangle$ for $a \in \mathbb{Z}$.

Example: The subgroups of $\mathbb{Z}_6$ are $\langle 0\rangle$, $\langle 3\rangle$, $\langle 2\rangle$, and $\langle 1\rangle = \mathbb{Z}_6$.



Theorem 1.24: Let $G = \langle a \rangle$ be cyclic with $|G| = n$. Then for any $k \in \mathbb{N}$, $\left|a^k\right| = \frac{n}{\gcd(n,k)}$.

Proof: Let $d = \gcd(n,k)$. We claim $\langle a^k \rangle = \langle a^d \rangle$.

($\subseteq$) Since $d|k$, $k = dq$ for some $q \in \mathbb{Z}$. Then $a^k = \left(a^d\right)^q \in \langle a^d \rangle$, so $\langle a^k \rangle \subseteq \langle a^d \rangle$.

($\supseteq$) By Bezout's identity, $d = ks + nt$ for some $s, t \in \mathbb{Z}$, so $a^d = a^{ks+nt} = \left(a^k\right)^s (a^n)^t = \left(a^k\right)^s (e)^t = \left(a^k\right)^s \in \langle a^k \rangle$. Thus $\langle a^d \rangle \subseteq \langle a^k \rangle$.

Now $\langle a^k \rangle = \langle a^d \rangle$, so in particular, $\left|a^k\right| = \left|a^d\right|$. We know $\left|a^d\right| = \frac{n}{d}$, since otherwise, if $\left|a^d\right| = m < \frac{n}{d}$, $a^{dm} = e$ amd $dm < n$, so $|G| = |a| < n$. $\lightning$ Thus $\left|a^k\right| = \left|a^d\right| = \frac{n}{d}$.

Corollary 1.24.1: Let $G = \langle a \rangle$ with $|G| = n$. Then the generators of G are a^k with $\gcd(k,n) = 1$.

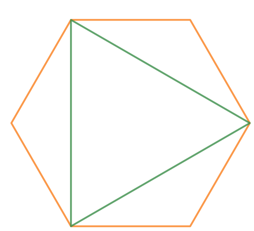
Proposition 1.25: Let G be a cyclic group and $a \in G$ such that $G \neq \langle a \rangle$. Then no element of $\langle a \rangle$ is a generator for G.

Proof: Suppose $|G| = n$. Since $\langle a \rangle \neq G$, $|a| < |G|$. Now every element of $\langle a \rangle$ is of the form a^k for some $k \in \mathbb{Z}$, and $\left|a^k\right| = \frac{|a|}{\gcd(k,|a|)} \leq |a| < |G|$, so no element of $\langle a \rangle$ is a generator for G.

Definition 1.26: Two groups G and H are **isomorphic** if there is a bijection $\varphi : G \longrightarrow H$ such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. φ is called an **isomorphism**, and we write $G \simeq H$.

Example: $\mathbb{Z}_4 \simeq \langle i \rangle \leq \mathbb{C}^*$, since the map $\varphi : \mathbb{Z}_4 \longrightarrow \angle i \rangle$ given by $\varphi(a) = i^a$ is an isomorphism.

Example: Let $H = \{x \in D_6 \mid x \text{ preserves an inscribed triangle}\} \leq D_6$. Then $H \simeq D_3$.



Proposition 1.27: Isomorphisms preserve identities, inverses, subgroups, and order (both of elements and groups).

II — The Symmetric Group

Definition 2.1: A ***k*-cycle** is an element of S_n of the form $(a_1 \cdots a_k)$.

Definition 2.2: A **transposition** is a 2-cycle.

Proposition 2.3: Every element of S_n can be expressed as a product of disjoint cycles.

Example: To remove duplicate numbers, start with 1 and pass it through the permutation, then pass the result through, and so on. Since every permutation is a bijection by definition, every number will be sent to a unique other. Once the permutation results in 1 again, close the cycle and continue with the next lowest unused number. For instance, if $\sigma = (124)(314)$, $\sigma(1) = 1$, so we start again with 2: $\sigma(2) = 4$. Then $\sigma(4) = 3$, and $\sigma(3) = 2$, so the permutation is (243).

Proposition 2.4: Disjoint cycles commute.

Proposition 2.5: Every element of S_n can be expressed as a product of transpositions.

Proof: For an arbitrary $\sigma \in S_n$, express σ as a product of disjoint cycles. Then for an individual cycle $(a_1 \cdots a_k)$, $(a_1 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$.

Definition 2.6: Let $\pi \in S_n$. The **permutation matrix** for π is P_π, defined by $(P_\pi)_{ij} = 1$ if $\pi(j) = i$ and 0 if not.

Example: For $\pi = (243) \in S_4$,

$$P_\pi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Proposition 2.7: All permutation matrices are orthogonal (that is, the columns form an orthonormal basis for $\mathbb{R}^n$, so $\det P_\pi = \pm 1$).

Definition 2.8: A permutation $\pi \in S_n$ is **even** if $\det P_\pi = 1$, and **odd** if $\det P_\pi = -1$.

Definition 2.9: The **alternating group** of degree n is $A_n = \{\pi \in S_n \mid \pi \text{ is even}\} \leq S_n$.

Proposition 2.10: For $n \geq 2$, $|A_n| = \frac{n!}{2}$.

Proof: Define $f : A_n \longrightarrow S_n \setminus A_n$ by $f(\pi) = (12)\pi$. Then $f^{-1}(\pi) = (12)\pi$, so f is invertible. Thus $|A_n| = |S_n \setminus A_n|$, so $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Theorem 2.11: Let $\pi \in S_n$. Then $\pi \in A_n$ if and only if π can be expressed as the product of evenly many transpositions. Moreover, when π is expressed in such a way, there are always the same number of transpositions (mod 2).

Proof: Suppose $\pi = \tau_1 \cdots \tau_k$, where each τ_i is a transposition. Then $P_\pi = P_{\tau_1} \cdots P_{\tau_k}$. Since P_{τ_i} has exactly 2 columns permuted from I_n, $\det P_{\tau_i} = -1$, so $\det P_\pi = (-1)^k$. Thus π is even if and only if k is even, proving both claims.

Theorem 2.12: Let $n \geq 3$. Then A_n is generated by 3-cycles.

Proof: Let $\pi \in A_n$. Then π is the product of evenly many transpositions. Group them in pairs, and consider an arbitrary pair, say $(ab)(cd)$.

If (ab) and (cd) have no common entries, then $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$ (which is valid, since $b \neq c$ by assumption).

If (ab) and (cd) have one entry in common, then without loss of generality, $(cd) = (bd)$. Then $(ab)(cd) = (ab)(bd) = (abd)$.

Finally, if (ab) and (cd) share two entries, they are identical, so $(ab)(cd) = e$. Thus each pair is expressible as either one or two 3-cycles or the identity, and since we can omit the identities, π is the product of 3-cycles.