# Discrete Math, Second series, 2nd Problem Set (July 21)

REU 2003

Instructor: Laszlo Babai
Scribe: Mridul Mehta

**Definition 0.1.** A **group** is a set $G$ with a binary operation $G \times G \to G$ denoted by '$\cdot$' or '$+$' depending on context, satisfying:

1. $(\forall\, x, y \in G)(\exists!\, z \in G)(x \cdot y = z)$
2. $(\forall\, x, y, z \in G)((x \cdot y) \cdot z = x \cdot (y \cdot z))$
3. $(\exists\, 1_G)(\forall\, x \in G)(x \cdot 1_G = 1_G \cdot x = 1_G)$
4. $(\forall\, x \in G)(\exists\, x^{-1} \in G)(x \cdot x^{-1} = x^{-1} \cdot x = 1_G)$

**Definition 0.2.** We say that $H \subseteq G$ is a **subgroup** of $G$ (written $H \leq G$) if

1. $1_G \in H$
2. $(\forall\, x, y \in H)(x \cdot y \in H)$
3. $(\forall\, x \in H)(x^{-1} \in H)$

**Exercise 0.3.** $G$ has no subgroups other than $\{1\}$ and $G \iff |G| = 1$ or $|G|$ is prime.

**Definition 0.4.** The **order** of a group is the number of elements it contains, and is denoted $|G|$.

**Theorem 0.5 (Lagrange).** *If $G$ is finite and $H \leq G$, then $|H|$ divides $|G|$.*

**Remark 0.6.** The union of two subgroups is in general, not a subgroup. (Consider $2\mathbb{Z}$ and $3\mathbb{Z}$ inside $(\mathbb{Z}, +)$.)

**Exercise 0.7.** If $H, K \leq G$, and $H \cup K \leq G$, then $H \subseteq K$ or $K \subseteq H$.

**Exercise 0.8.** Determine all (finite or infinite) groups for which the union any two of subgroups is a subgroup.

**Exercise 0.9.** The intersection of any set of subgroups is a subgroup.

**Definition 0.10.** **Subgroup generated by a subset** $S \subseteq G$ (written $\langle S \rangle$). There are two equivalent definitions:

1. $\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$
2. $\langle S \rangle = \{$ all products of generators and their inverses $\}$

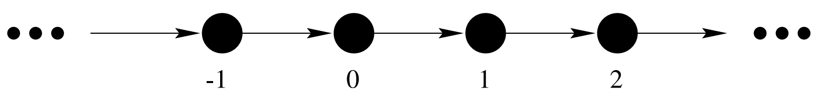
**Remark 0.11.** By convention, we have $\langle \emptyset \rangle = \{1\}$.

**Exercise 0.12.** Prove that the two definitions of $\langle S \rangle$ are equivalent.

A graph is an object with a given set of vertices (usually denoted $V$), which are connected by edges (denoted $E$). We usually denote the graph by $(V, E)$. A digraph is one in which the edges are directed (so that $E \subseteq V \times V$).

A **Cayley graph** $\Gamma$ of a group $G$ with respect to a given set of generators $S \subseteq G$ is the digraph $\Gamma(G, S) = (G, E_S)$, where $E_S = \{(g, sg) \colon g \in G, s \in S\}$.

**Example 0.13.** $G = (\mathbb{Z}, +) = \langle 1 \rangle$. The Cayley graph is:




For example, $(2, 3) \in E$ because $2 + 1 = 3$ and $1 \in S$.

**Definition 0.14.** A group $G$ is said to be **cyclic** if $\exists\, a \in G$ such that $G = \langle a \rangle$.

**Definition 0.15.** The **order** of an element $x \in G$ (denoted by $\mathrm{ord}(x)$) isdefined as the order of the cyclic subgroup generated by $x$ i.e. $\mathrm{ord}(x) = |\langle x \rangle|$. (So $\mathrm{ord}(x) = k \Rightarrow 1, x, \ldots, x^{k-1}$ are distinct and $x^k = 1$. Moreover, $x^i = x^j \iff i \equiv j \mod k$.)

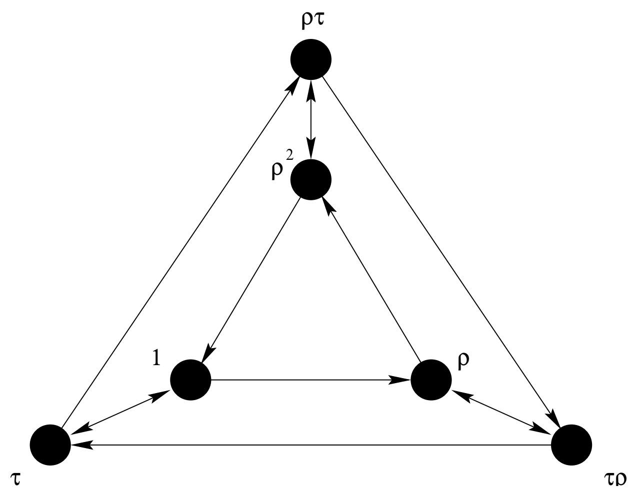
**Exercise 0.16.** Suppose $G$ is a **abelian** group (i.e. operation is commutative). If $x, y \in G$ such that $\mathrm{ord}(x) = a$ and $\mathrm{ord}(y) = b$, then prove that g.c.d. $(a, b) = 1 \Rightarrow \mathrm{ord}(xy) = ab$.

**Exercise 0.17.** Suppose $G$ is a abelian group. If $x, y \in G$ such that $\mathrm{ord}(x) = a$ and $\mathrm{ord}(y) = b$, then prove that

$$\frac{\text{l.c.m.}\,(a, b)}{\text{g.c.d.}\,(a, b)} \mid \mathrm{ord}(xy) \mid \text{l.c.m.}\,(a, b).$$

The **Dihedral group** of order $2n$, denoted $D_n$, is the group of symmetries (rotations and reflections) of the regular $n$-gon in the plane.

**Example 0.18.** $|D_3| = 6$ (group of symmetries of an equilateral triangle in the plane). If we denote the reflections by $\tau_1, \tau_2, \tau_3$ and the rotations by $1, \rho, \rho^2$ ($\rho^3 = 1$), then $D_3 = \langle \rho, \tau_1 \rangle$. Consequently its Cayley graph is:




The edges comprising the triangles correspond to multiplication by $\rho$ while the two-way arrows correspond to multiplication by $\tau$ (since $\tau$ has order 2). Following a directed edge in the opposite direction corresponds to multiplication by the inverse of the element. Each path corresponds to multiplying by the generators and/or their inverses in a particular order.

**"Relation chasing"** Two different paths between the same pair of vertices give rise to two different expressions for the same group element as products of generators and their inverses. In particular, closed walks specify products of generators which equal the identity. Such products are called **relations** among the generators. For example, the inner triangle, from the identity to itself, shows the relation $\rho^3 = 1$. The walk of length 2 from 1 to $\tau$ to 1 shows that $\tau^2 = 1$. Traversing the bottom quadrilateral clockwise shows the relation $\tau\rho\tau\rho = 1$. A more complex relation that is immediate from the diagram is $\rho\tau\rho^2\tau\rho = 1$.

**Definition 0.19.** A **homomorphism** from a group $G$ to a group $H$ is a map $f : G \to H$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$.

**Remark 0.20.**

1. $f(1_G) = 1_H$.
2. $f(x^{-1}) = f(x)^{-1}$.
3. $f^{-1}(1_H) \leq G$. The subgroup $f^{-1}(1_H)$ is called the **kernel** of $f$, denoted $\ker(f)$.

For any $g \in G$, "**conjugation** by $g$" means a map $G \to G$ given by $x \mapsto g^{-1}xg =: x^g$. Note that $\ker(f)$ is always closed under conjugation.

**Definition 0.21.** A subgroup $N \leq G$ is called a **normal subgroup** if it is closed under conjugation, i. e., $(\forall\, g \in G)(N^g = N)$. We write $N \triangleleft G$. (Here $N^g = \{n^g : n \in N\}$.)

**Definition 0.22.** We say that a map $f : G \to H$ is an **isomorphism** if $f$ is a homomorphism that is both injective (one-to-one) and surjective (onto). We say $G$ and $H$ are **isomorphic** (notation: $G \cong H$) if $\exists f : G \to H$ isomorphism.

**Definition 0.23.** An **automorphism** of a group $G$ is an isomorphism from $G \to G$.

**Exercise 0.24.** Conjugation by any $g \in G$ ($x \mapsto x^g$) is an automorphism of $G$. Such automorphisms (induced by conjugation) are known as **inner automorphisms**.

The automorphisms of $G$ form a group under composition, called $\mathrm{Aut}(G)$.

**Example 0.25.** $\mathrm{Aut}(\mathbb{Z}, +) \cong (\mathbb{Z}_2, +)$.

**Exercise 0.26.** Prove that $(\mathbb{Z}_n^\times, \cdot)$ is a group. This is the multiplicative group of integers modulo $n$ that are relatively prime to $n$. The order of this group is $\phi(n)$ (Euler's phi function) see Basic Number Theory handout, Section 4.2.

**Example 0.27.** $\mathrm{Aut}(\mathbb{Z}_n, +) \cong (\mathbb{Z}_n^\times, \cdot\ )$.

**Exercise 0.28.** $\mathrm{ord}(k)$ (in $(\mathbb{Z}_n, +)$) $= \frac{n}{\text{g.c.d.}\,(k,n)}$.

**Exercise 0.29.** $\mathrm{ord}(g^k)$ (in group $G$) $= \frac{\mathrm{ord}(g)}{\text{g.c.d.}\,(k,\mathrm{ord}(g))}$.

**Exercise$^+$ 0.30.** The group $(\mathbb{Z}_n^\times, \cdot\ )$ is cyclic if and only if

- $n$ is prime or
- $n = p^k$ for some odd prime $p$ or
- $n = 2p^k$ for some odd prime $p$.

**Definition 0.31. Direct Product**. Given groups $G$, $H$, their Cartesian product $G \times H = \{(g, h) \colon g \in G, h \in H\}$ is a group under componentwise multiplication.

**Example 0.32.** $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{1, a, b, c\}$, where $a^2 = b^2 = c^2 = 1$, $ab = c, ac = b, bc = a$, and the group is abelian. This is known as Klein's 4-group and is usually denoted by $V_4$.

**Exercise 0.33.** Prove that $\mathbb{Z}_8^\times \cong V_4$.

**Exercise 0.34.** The only groups (up to isomorphism) of order 4 are $\mathbb{Z}_4$ and $V_4$.

**Exercise 0.35.** Find all $n$ such that $\mathbb{Z}_n^\times \cong V_4$.

**Definition 0.36.** The **center** of a group $G$, is defined to be $Z(G) = \{a \in G \colon (\forall g \in G)(ga = ag)\}$.

**Exercise 0.37.** Find $Z(D_n)$.

We consider the map from $G \to \mathrm{Aut}(G)$ given by $g \mapsto \{x \mapsto x^g\}$. This is a homomorphism of groups. The kernel of this map is $Z(G)$. The image of this map is the **group of inner automorphisms** of $G$, denoted by $\mathrm{Inn}(G)$.

**Exercise 0.38.** Prove that $G/Z(G) \cong \mathrm{Inn}(G)$.

**Exercise 0.39.** Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is also denoted by $\mathrm{Out}(G)$, and referred to as the **outer automorphism group** of $G$.

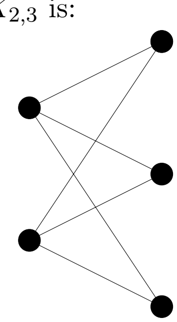
**Definition 0.40. Symmetric group of degree n**. This is the group of all permutations of a set of $n$ elements under composition. It is usually denoted by $S_n$. Clearly, $|S_n| = n!$.

**Remark 0.41.** The group $S_n$ has an important subgroup $A_n$, known as the **alternating group** of degree $n$ which consists of the even permutations of degree $n$. For $n \geq 2$, $|A_n| = \frac{n!}{2}$.

**Exercise 0.42.** Prove that $Z(S_n) = \{1\}$ for $n \geq 3$ and $Z(A_n) = \{1\}$ for $n \geq 4$.

**Definition 0.43. Bipartite graph**. The bipartite graph $K_{p,q}$ is a graph with $p + q$ vertices partitioned into two sets of $p$ and $q$ vertices respectively such that no two vertices in the same set are adjacent, while every pair of vertices not in the same set are adjacent.

**Example 0.44.** The bipartite graph $K_{2,3}$ is:



**Exercise 0.45.** Suppose $G = \langle S\rangle$, where $S$ is minimal in the sense that $(\forall\, T \subsetneq S)(\langle T\rangle \neq G)$. Prove that $\Gamma(G, S \cup S^{-1}) \not\supseteq K_{3,5}$.