ABEL'S THEOREM-1. GROUPS.

We expect the notions of a set, a map (of sets), and a composition of maps to be familiar.

DEFINITION 1. We say that a map $f : X \to Y$ is *surjective* if every element of Y has a preimage, *injective* if no two elements of X have the same image, and *bijective*, or *one-to-one*, if it is both surjective and injective, thus establishing a one-to-one correspondence between elements of X and Y. We will refer to a bijective map $X \to X$ as a *transformation* of X. We denote the identity transformation by id.

1.1. Which of the following maps $\mathbb{Z} \to \mathbb{Z}_{\geq 0}$ are injective, surjective, or bijective? **a)** $n \mapsto |n|$; **b)** $n \mapsto 2n$ if $n \geq 0$, and $n \mapsto -1 - 2n$ if $n < 0$; **c)** $n \mapsto n^2$; **d)** $n \mapsto n^2$ if $n \geq 0$, and $n \mapsto n^2 + 1$ if $n < 0$.

1.2. Let f be a map $f : X \to Y$. Prove that

- **a)** the map f is injective if and only if there is a map $g : Y \to X$ such that $g \circ f = id_X$.
- **b)** the map f is surjective if and only if there is a map $g : Y \to X$ such that $f \circ g = id_Y$.
- **c)** the map f is bijective if and only if there is a map $g : Y \to X$ such that $g \circ f = id_X$ and $f \circ g = id_Y$. In this case g is called *the inverse map* for f.

DEFINITION 2. A transformation of a geometrical figure is called a *symmetry*, if it preserves all distances between points of the figure.

1.3. Introduce the notation and write the multiplication table for symmetries of **a)** an equilateral triangle **b)** a square **c)** a rectangle that is not a square.

DEFINITION 3. A *group of transformations* is a set S of transformations possessing the following two properties: 1) for any $g_1, g_2 \in S$, $g_1 g_2 \in S$; 2) for any $g \in S$, $g^{-1} \in S$.

1.4. Let G be a group of transformations. Prove that

- **a)** $id \in G$;
- **b)** for any $g \in G$ $\quad id \circ g = g \circ id = g$;
- **c)** for any $g_1, g_2, g_3 \in G$, we have $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$.

DEFINITION 4. For a set X, the *direct product* $X \times X$ is the set of all pairs of elements of X: $X \times X = \{(x, y) | x, y \in X\}$. A *binary operation* on a set X is a map $X \times X \to X$. A set G with a binary operation $m : G \times G \to G$ is a *group*, if the following conditions are satisfied:

(1) there is an element $e \in G$ (called *the identity*) such that for all $g \in G$, $m(g, e) = m(e, g) = g$;
(2) for all $g_1, g_2, g_3 \in G$, $m(m(g_1, g_2), g_3) = m(g_1, m(g_2, g_3))$;
(3) for each $g \in G$ there is $f \in G$ (called the *inverse* of g and denoted g^{-1}) such that $m(g, f) = m(f, g) = e$.

We will simply write fg for $m(f, g)$ from now on.

1.5. Which of the following sets make a group under addition? Under multiplication?
a) $\mathbb{Z}$ **b)** $\mathbb{Z}_{\geq 0}$ **c)** $\mathbb{R}$ **d)** $\mathbb{R} - \{0\}$

1.6. Prove that the identity in a group is unique.

1.7. Prove that for any element of a group its inverse element is unique.

1.8. Prove that in any group
a) $e^{-1} = e$; **b)** $(a^{-1})^{-1} = a$ **c)** $(ab)^{-1} = b^{-1}a^{-1}$.

1.9. Prove that in any group the equation $ax = b$ (resp. $xa = b$) has a unique solution for any a and b.

DEFINITION 5. Let G be a group. For each $g \in G$ the *order* of g is the smallest positive integer n such that $g^n = e$. If there is no such integer, we say that g has *infinite order*. A group G is called *cyclic* of order n, if it consists of all integral powers of an element $g \in G$ of order n. The element g is called a *generator* of G. Note that a cyclic group can have several generators.

1.10. Let the order of an element g of G be n. Prove that $g^m = e$ if and only if $m = kn$, $k \in \mathbb{Z}$.

1.11. Prove that rotations of a regular n-gon form a cyclic group, and find all generators of the group of rotations of a regular dodecagon ($n = 12$).

1.12. Prove that $\mathbb{Z}$ is a cyclic group under addition and find all its generators.

1.13. Denote by $\mathbb{Z}_n$ the set of all possible remainders modulo n: $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Define a binary operation on $\mathbb{Z}_n$ as addition modulo n. Prove that $\mathbb{Z}_n$ is a cyclic group of order n.

1.14. Prove that $k \in \mathbb{Z}_n$ is a generator if and only if $\gcd(k, n) = 1$.

DEFINITION 6. Let G_1 and G_2 be two groups. A bijection $\phi : G_1 \to G_2$ is an *isomorphism of groups*, if for any $g_1, g_2 \in G_1$ we have $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. Two groups are *isomorphic* if there is an isomorphism between them. In this case we write $G \simeq H$.

1.15. Let $\phi : G \to H$ be an isomorphism of groups. Prove that **a)** $\phi(e_G) = e_H$;
b) $\forall g \in G\ \phi(g^{-1}) = \phi(g)^{-1}$; **c)** for all $g \in G$ the element $\phi(g)$ has the same order as the element g.

1.16. Let $\phi : G \to H$ be an isomorphism of groups. By definition, ϕ is a bijection, so there is an inverse map ϕ^{-1}. Prove that ϕ^{-1} is an isomorphism of groups as well.

1.17. Prove that any cyclic group generated by an element of finite order n is isomorphic to $\mathbb{Z}_n$, and any cyclic group generated by an element of infinite order is isomorphic to $\mathbb{Z}$.

1.18. Give an example of two non-isomorphic groups with the same number of elements.

1.19. Prove that the group of all real numbers under addition is isomorphic to the group of all positive real numbers under multiplication.

1.20. Let G be a group. To any element $g \in G$ we can associate two transformations of G itself: a transformation $\phi_g : G \to G$ that sends $h \in G$ to gh, and a transformation $\psi_g : G \to G$ that sends $h \in G$ to hg^{-1}. Prove that the set Φ of all ϕ_g and the set Ψ of all ψ_g (for all $g \in G$) both form groups isomorphic to G.

Note that while Φ and Ψ are both subsets of the set of transformations of G, they generally don't coincide.

DEFINITION 7. Let G be a group. A subset of G that forms a group under the same binary operation is called a *subgroup* of G. If $S \subset G$ is a subset, we can define *the subgroup of G generated by S* as a minimal subgroup that contains S, or, equivalently, as the set of all possible products of any (finite) number of elements of S and their inverses. Note that a subgroup generated by a single element is a cyclic group.

1.21. Let G be a group. Prove that $H \subset G$ is a subgroup if and only if the following three conditions hold:

(1) $e \in H$;
(2) if $a, b \in H$, then $ab \in H$; (in this case we say that H is closed under the group operation)
(3) if $a \in H$, then $a^{-1} \in H$.

1.22. Prove that any subgroup of a cyclic group is cyclic. (Hint: consider the cases of a finite and an infinite cyclic groups separately, and use problem 1.17.)

1.23. Prove that for every m dividing n there is a unique subgroup of $\mathbb{Z}_n$ isomorphic to $\mathbb{Z}_m$.

1.24. Prove that the intersection of an arbitrary number of subgroups of G is itself a subgroup.

1.25. Find the number of elements of the group S of symmetries of a regular tetrahedron.

1.26. Prove that all symmetries that preserve the orientation of a regular tetrahedron (i.e. are compositions of rotations around some axes) form a subgroup R of the group S, and find the number of elements in this subgroup.

1.27. Consider a regular tetrahedron with vertices A, B, C, D. Let us write $\begin{pmatrix} A & B & C & D \\ B & D & C & A \end{pmatrix}$ for a symmetry of the tetrahedron that takes A to B, B to D, C to C, and D to A. In this case the symmetry is the rotation by 120° around the axis that passes through C and the center of symmetry. Using this notation, describe all subgroups of **a)** S **b)** R up to isomorphism.

1.28. Prove that if G and H are groups, than $G \times H$ with the binary operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ is a group. This group is called *the direct product of groups G and H*.

This is not the only way to define a binary operation on the set $G \times H$, so the words "direct product" here refer specifically to group structures: the above group structure on $G \times H$ is the direct product of the group structure on G and the group structure on H.

1.29. Prove that $G \times H \simeq H \times G$.

1.30. Prove that if G_1 is a subgroup of G and H_1 is a subgroup of H, then $G_1 \times H_1$ is a subgroup of $G \times H$. In particular, when $G_1 = G$ and $H_1 = \{e_H\}$, there is the subgroup $G \times \{e_H\}$ isomorphic to G (and, similarly, the subgroup $\{e_G\} \times H$ isomorphic to H).

EXAMPLE 1. Not all subgroups of $G \times H$ are of the form $G_1 \times H_1$ for $G_1 \subset G$, $H_1 \subset H$. For example, the subgroup $\Delta = \{(n, n) | n \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$ is not of this form.

1.31. Find all subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

1.32. Prove that $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if and only if m and n are relatively prime.