Problem 1

In this problem, no explanation is required. All parts are worth 2 points.

(a) True or false: In a free abelian group of finite rank, every linearly independent set can be completed to a basis.

(b) How many different (up to isomorphism) abelian groups of order 300 are there?

(c) True or false: For any action of a finite group G on a set X, the cardinality $|X|$ divides $|G|$.

(d) Give an example of an infinite group G such that every element of G has finite order.

(e) Let F_2 be the free group on two generators. True or false: For every n, there exists a normal subgroup $H_n \subset F_2$ such that $F_2/H_n \cong S_n$?

(a) True.

(b) There are 4 abelian groups of order 300 up to isomorphism.

(c) False.

(d) An example of an infinite group where every element has finite order is the group of all roots of unity in the complex numbers, denoted by $\{e^{2\pi ik/n} \mid k \in \mathbb{Z}, n \in \mathbb{N}\}$.

(e) True.

Problem 2

Let $\mathbb{Q}^\times$ be the group of non-zero rational numbers under multiplication.

(a) Show that $\mathbb{Q}^\times$ is isomorphic to the product of $\mathbb{Z}/2\mathbb{Z}$ and a free abelian group.

(b) Describe all group homomorphisms $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}^\times$.

(c) Describe all group homomorphisms $\mathbb{Q}^\times \to \mathbb{Z}/2\mathbb{Z}$.

(a) *Proof.* By the Fundamental Theorem of Arithmetic, every non-zero rational number can be uniquely expressed as a product of prime numbers raised to integer powers. Specifically, any $q \in \mathbb{Q}^\times$ can be written as

$$q = \pm p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where p_i are distinct prime numbers and $a_i \in \mathbb{Z}$. The sign of q can be captured by the factor ± 1, which corresponds to the group $\mathbb{Z}/2\mathbb{Z}$. To see this, note that the group $\mathbb{Z}/2\mathbb{Z}$ has two elements: the identity element 0 (which corresponds to $+1$) and the non-identity element 1 (which corresponds to -1). Thus, we can separate the sign from the rest of the rational number.
The remaining part, $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, forms a free abelian group generated by the primes. To see that this is a free abelian group, note that the exponents a_i can be any integers, and the multiplication of rational numbers corresponds to the addition of these exponents. Thus, we can express $\mathbb{Q}^\times$ as the direct product

$$\mathbb{Q}^\times \cong \mathbb{Z}/2\mathbb{Z} \times F,$$

where F is the free abelian group generated by the primes. Therefore, we conclude that $\mathbb{Q}^\times$ is isomorphic to the product of $\mathbb{Z}/2\mathbb{Z}$ and a free abelian group. □

(b) The group $\mathbb{Z}/2\mathbb{Z}$ has two elements: 0 and 1. The image of the identity element 0 must be the identity element in $\mathbb{Q}^\times$, which is 1. The image of the non-identity element 1 can either be 1 or -1. Thus, there are two possible homomorphisms: the trivial homomorphism sending both elements to 1, and the homomorphism sending 0 to 1 and 1 to -1.

(c) Any homomorphism $\varphi : \mathbb{Q}^\times \to \mathbb{Z}/2\mathbb{Z}$ must satisfy $\varphi(xy) = \varphi(x) + \varphi(y)$ for all $x, y \in \mathbb{Q}^\times$. We have found that $\mathbb{Q}^\times$ is generated by -1 and the prime numbers so any homomorphism id determined by its values on these generators.
Then we have that $\varphi(-1) \in \mathbb{Z}/2\mathbb{Z}$ can be either 0 or 1. For any prime number p, we have that $\varphi(p^n) = n\varphi(p)$ for any integer n. Since $\mathbb{Z}/2\mathbb{Z}$ has only two elements, $\varphi(p)$ can also be either 0 or 1. Thus, for each prime number, we have two choices for its image under φ.
Therefore, the group homomorphisms from $\mathbb{Q}^\times$ to $\mathbb{Z}/2\mathbb{Z}$ are determined by the choices of images for -1 and each prime number, leading to a large number of possible homomorphisms. $\mathrm{Hom}(\mathbb{Q}^\times, \mathbb{Z}/2\mathbb{Z}) \cong \bigoplus_{p \text{ prime}} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The additional $\mathbb{Z}/2\mathbb{Z}$ factor corresponds to the choice of image (sign) for -1.

Problem 3

Let G be a group of order $2017 \times 2027 \times 2029$ (these are all prime numbers). Show that G is cyclic.

Proof. We have that the order of G is the product of three distinct primes: 2017, 2027, and 2029. Then, by the first Sylow theorem, for each prime p dividing the order of G, there exists a Sylow p-subgroup of G. Let n_p denote the number of Sylow p-subgroups of G. By the third Sylow theorem, we have that $n_p \equiv 1 \mod p$ and n_p divides the order of G. Since the primes are distinct and large, the only divisors of the order of G that are congruent to 1 modulo p are 1 itself. Therefore, each Sylow p-subgroup is unique and hence normal in G. Since the Sylow subgroups are normal and their orders are pairwise relatively prime, G is isomorphic to the direct product of its Sylow subgroups, each of which is cyclic of prime order. Thus, we have that $G = \mathbb{Z}/2017\mathbb{Z} \times \mathbb{Z}/2027\mathbb{Z} \times \mathbb{Z}/2029\mathbb{Z}$ is cyclic. □

Problem 4

Let G be a finite group, and let $A = \mathrm{Aut}(G)$ be the group of automorphisms $\phi : G \to G$. Consider the natural action of A on G, and take the quotient G/A.

(a) What is $|G/A|$ if $G = \mathbb{Z}/6\mathbb{Z}$?

(b) Show that if $|G/A| = 2$, then $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ for a prime p and $n > 0$.

(a) For $G = \mathbb{Z}/6\mathbb{Z}$, the automorphism group $\mathrm{Aut}(G)$ consists of all group automorphisms of $\mathbb{Z}/6\mathbb{Z}$. The elements of $\mathbb{Z}/6\mathbb{Z}$ are $\{0, 1, 2, 3, 4, 5\}$. The automorphisms are determined by the images of the generator 1. The possible images are 1 and 5 (since they are coprime to 6). Thus, there are two automorphisms: the identity and the one sending 1 to 5. The orbits under this action are $\{0\}$, $\{1, 5\}$, $\{2, 4\}$, and $\{3\}$. Therefore, there are 4 distinct orbits, so $|G/A| = 4$.

(b) *Proof.* We have that $|G/A| = 2$ implies that there are exactly two orbits under the action of $\mathrm{Aut}(G)$ on G. One orbit must be the identity element $\{e\}$, and the other orbit must contain all other elements of G. This means that for any non-identity element $g \in G$, there exists an automorphism $\phi \in \mathrm{Aut}(G)$ such that $\phi(g) = h$ for any other non-identity element $h \in G$. This property implies that all non-identity elements of G have the same order. Let this common order be p. Since G is finite, p must be a prime number. Thus, every non-identity element of G has order p, and G is a p-group. Furthermore, since all non-identity elements have the same order, G must be isomorphic to a direct product of copies of $\mathbb{Z}/p\mathbb{Z}$. Therefore, we conclude that $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ for some prime p and integer $n > 0$. □

Problem 5

A finite group G acts transitively (that is, with a single orbit) on a finite set X such that $|X| > 1$. Show that there exists an element $g \in G$ which does not fix any element of X.

Proof. Let G act transitively on the set X. By Theorem II.4.3, the size of the orbit of any element $x \in X$ under the action of G is given by the index $[G : G_x]$, where G_x is the stabilizer of x in G. Since the action is transitive, there is only one orbit, which means that the size of the orbit is equal to the size of the set X, denoted as $|X|$.

Now, since $|X| > 1$, we have $|X| = [G : G_x] > 1$. This implies that the index $[G : G_x]$ is greater than 1, meaning that the stabilizer G_x is a proper subgroup of G.

By Lagrange's theorem, the order of G is equal to the order of the stabilizer G_x multiplied by the size of the orbit, i.e.,

$$|G| = |G_x| \cdot |X|.$$

Since $|X| > 1$, it follows that $|G| > |G_x|$.

Now, consider the action of G on the set X. If every element of G fixed every element of X, then the action would be trivial, meaning that every element of G would act as the identity on X. However, this contradicts the fact that the action is transitive and that $|X| > 1$.

Therefore, there must exist at least one element $g \in G$ such that g does not fix any element of X. This means that for every $x \in X$, we have $g \cdot x \neq x$.

Thus, we conclude that there exists an element $g \in G$ which does not fix any element of X. □

Problem 6

A map $\phi : \mathbb{R} \to \mathbb{R}$ is said to be an *affine-linear bijection* if it is of the form

$$\phi(x) = ax + b \quad (a, b \in \mathbb{R} : a \neq 0).$$

(a) Show that the set of affine-linear bijections forms a group G under composition.

(b) Show that G is isomorphic to semidirect product of *abelian* groups A and B. Make sure to identify the groups A and B, as well as the action of one on the other used in the semidirect product.

(a) *Proof.* To show that the set of affine-linear bijections forms a group under composition, we show closure, associativity, identity, and inverses.
First we show closure. Let $\phi(x) = ax + b$ and $\psi(x) = cx + d$ be two affine-linear bijections. Then their composition is given by

$$(\phi \circ \psi)(x) = \phi(\psi(x)) = a(cx + d) + b = (ac)x + (ad + b),$$

which is again of the form $ex + f$ with $e = ac \neq 0$. Thus, the composition of two affine-linear bijections is again an affine-linear bijection, establishing closure.
Next we show associativity. Let $\phi(x) = ax + b$, $\psi(x) = cx + d$, and $\theta(x) = ex + f$ be three affine-linear bijections. Then we have

$$\begin{aligned}((\phi \circ \psi) \circ \theta)(x) &= (\phi \circ \psi)(\theta(x)) = \phi(\psi(ex + f)) = \phi(c(ex + f) + d) = a(c(ex + f) + d) + b \\ &= acex + acf + ad + b, \\ (\phi \circ (\psi \circ \theta))(x) &= \phi((\psi \circ \theta)(x)) = \phi(\psi(ex + f)) = \phi(c(ex + f) + d) = a(c(ex + f) + d) + b \\ &= acex + acf + ad + b.\end{aligned}$$

Clearly $((\phi \circ \psi) \circ \theta)(x) = (\phi \circ (\psi \circ \theta))(x)$, thus we have associativity.
Next we show the identity element. From intuition, we can see that the identity element should be $\mathrm{id}(x) = x$. To verify this, let $\phi(x) = ax + b$ be an affine-linear bijection. Then we have

$$(\phi \circ \mathrm{id})(x) = \phi(\mathrm{id}(x)) = \phi(x) = ax + b,$$

and

$$(\mathrm{id} \circ \phi)(x) = \mathrm{id}(\phi(x)) = \phi(x) = ax + b.$$

Thus, id is the identity element.
Finally, we show the existence of inverses. For $\phi(x) = ax + b$, the inverse is given by

$$\phi^{-1}(x) = \frac{1}{a}x - \frac{b}{a},$$

which can be verified as follows:

$$(\phi \circ \phi^{-1})(x) = \phi\left(\frac{1}{a}x - \frac{b}{a}\right) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x - b + b = x = \mathrm{id}(x),$$

and

$$(\phi^{-1} \circ \phi)(x) = \phi^{-1}(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x + \frac{b}{a} - \frac{b}{a} = x = \mathrm{id}(x).$$

Thus, every affine-linear bijection has an inverse that is also an affine-linear bijection.
Since we have shown closure, associativity, identity, and inverses, we conclude that the set of affine-linear bijections forms a group under composition. □

(b) *Proof.* We can identify the group A as the group of translations, which consists of all affine-linear bijections of the form $\phi(x) = x + b$ for $b \in \mathbb{R}$. This group is isomorphic to $(\mathbb{R}, +)$, which is abelian.
The group B can be identified as the group of dilations, which consists of all affine-linear bijections of the form $\psi(x) = ax$ for $a \in \mathbb{R}^\times$ (the non-zero real numbers). This group is also abelian under multiplication.
The action of B on A is given by conjugation. Specifically, for $\psi(x) = ax \in B$ and $\phi(x) = x + b \in A$, we have

$$\psi \circ \phi \circ \psi^{-1}(x) = a(x + b/a) = ax + b,$$

which shows that the action of B on A scales the translation by the factor a.
Therefore, we can express the group G of affine-linear bijections as the semidirect product of A and B, denoted by $G \cong A \rtimes B$. This establishes that G is isomorphic to the semidirect product of the abelian groups A and B. □