MATH 150A Winter 2020 - **Problem Set 2 solutions**

due January 24

1. (a) Characterize the elements of $\mathbb{C}^\times$ that have order n for positive integer n.

   The elements of order n are $e^{2\pi i \frac{a}{n}}$ where a is an integer with $\gcd(a, n) = 1$.

   (b) Characterize the elements of $\mathbb{C}^\times$ that have order ∞.

   The elements of order ∞ are all of the elements z not of the above form for any n. So either $|z| \neq 1$ or $z = e^{2\pi i r}$ for r an irrational number.

2. (2.4.3) Let a and b be elements of a group G. Prove that ab and ba have the same order.

   Suppose that $(ab)^n = 1$ for some positive integer n. Multiply both sides of the equation by a^{-1} on the left and by a on the right

$$a^{-1}(abab \cdots ab)a = a^{-1}1a,$$

$$bab \cdots aba = 1,$$

$$(ba)^n = 1.$$

   Conversely, suppose $(ba)^n = 1$. Multiplying both sides of the equation by b^{-1} on the left and by b on the right gives $(ab)^n = 1$. Therefore $(ab)^n = 1$ if and only if $(ba)^n = 1$. If the order of ab is finite, it is the smallest positive integer n such that $(ab)^n = 1$, which is also the smallest positive integer n such that $(ba)^n = 1$. If the order of ab is ∞, then $(ab)^n \neq 1$ for all postive integers n, and the same is true for $(ba)^n$ so ba also has order ∞.

3. (2.4.10) Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian?

   There are various sources of examples, but one comes from the permutation group of $\mathbb{Z}$, which is the group of invertible functions $\mathbb{Z} \to \mathbb{Z}$.

   Let $f : \mathbb{Z} \to \mathbb{Z}$ be the function that swaps each even integer with the following odd integer, so $f(2a) = 2a + 1$ and $f(2a + 1) = 2a$ for all $a \in \mathbb{Z}$. Let $g : \mathbb{Z} \to \mathbb{Z}$ be the function that swaps each even integer with the previous odd integer, so $g(2a) = 2a - 1$ and $g(2a - 1) = 2a$ for all $a \in \mathbb{Z}$. It is easy to see that both f and g have order 2, meaning that both $f \circ f$ and $g \circ g$ are equal to the identity function, since they consist of swaps.

   The composition $g \circ f : \mathbb{Z} \to \mathbb{Z}$ is the function defined by $g \circ f(2a) = 2a + 2$ and $g \circ f(2a + 1) = 2a - 1$ for all $a \in \mathbb{Z}$. This function has infinite order since $(g \circ f)^n(2a) = 2a + 2n$ which is not equal to $2a$ for any positive integer n.

   If the group is abelian, then the product of elements of finite order must also have finite order. Suppose x has order n and y has order m. Then

$$(xy)^{nm} = x^{nm}y^{nm} = (x^n)^m(y^m)^n = 1^m1^n = 1$$

   so xy has finite order.

4. (2.5.2) Let H and K be subgroups of group G.

   (a) Prove that the intersection $K \cap H$ is a subgroup of H.

   Suppose $a, b \in K \cap H$. Since K and H are subgroups, $ab^{-1} \in K$ and $ab^{-1} \in H$, so $ab^{-1} \in K \cap H$. Therefore $K \cap H$ is a subgroup.

   (b) Prove that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.

   Suppose that K is a normal subgroup, so for all $k \in K$ and $g \in G$, $gkg^{-1} \in K$. Then for all $k \in K \cap H$ and $g \in H$, $gkg^{-1} \in K$. Since k, g, g^{-1} are all in H, $gkg^{-1} \in H$, so $gkg^{-1} \in K \cap H$. Therefore $K \cap H$ is a normal subgroup of H.

5. (a) Find an injective homomorphism from the symmetric group S_3 to $\mathrm{GL}_3(\mathbb{R})$.

   Let e_1, e_2, e_3 denote the standard basis vectors of $\mathbb{R}^3$. Each permutation $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ can be mapped to the linear transformation T_σ that permutes the standard basis vectors according to σ, so $T_\sigma(e_i) = e_{\sigma(i)}$. The matrix representation of T_σ is called a permutation matrix. For S_3, the permutation matrices are

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}, \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}, \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}, \begin{bmatrix}0&1&0\\0&0&1\\1&0&1\end{bmatrix}, \begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}, \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}.$$

   (b) Let C_8 denote the cyclic group of order 8. Find an injective homomorphism from C_8 to $\mathrm{GL}_2(\mathbb{R})$.

   The cyclic group can be mapped to rotations of $\mathbb{R}^2$, with the generator x of C_8 sent to one eighth of a full turn. This map is $f : C_8 \to \mathrm{GL}_2(\mathbb{R})$ with

$$f(x^k) = \begin{bmatrix}\cos(k\pi/4) & -\sin(k\pi/4)\\ \sin(k\pi/4) & \cos(k\pi/4)\end{bmatrix}.$$

6. (2.5.4) Let $f : \mathbb{R}^+ \to \mathbb{C}^\times$ be the map defined by $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.

   For all $x, y \in \mathbb{R}$,

$$f(x+y) = e^{i(x+y)} = e^{ix}x^{iy} = f(x)f(y).$$

   Therefore f is a group homomorphism. The image of f is the complex unit circle

$$\mathrm{im}(f) = \{z \in \mathbb{C} \mid |z| = 1\}.$$

   The kernel is the set of real numbers x such that $e^{ix} = 1$, which is

$$\ker(f) = \{2\pi n \mid n \in \mathbb{Z}\} = 2\pi\mathbb{Z}.$$

7. Let D_5 denote the *dihedral group of the pentagon*, which is the group of order 10 consisting of the symmetries of a regular pentagon in the plane. D_5 is generated by r and s which represent a counter-clockwise rotation of the pentagon by $2\pi/5$ radians, and a reflection, respectively. Find all subgroups of D_5 and determine which subgroups are normal.

   The elements of D_5 can be represented in terms of generators as $1, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s$. Then the subgroups of D_5 are

- $\{1\}$
- $\{1, s\}$
- $\{1, rs\}$
- $\{1, r^2s\}$
- $\{1, r^3s\}$
- $\{1, r^4s\}$
- $\{1, r, r^2, r^3, r^4\}$
- $\{1, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$

The normal subgroups are

- $\{1\}$
- $\{1, r, r^2, r^3, r^4\}$
- $\{1, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$

8. (a) Prove that if $f : \mathbb{Q}^+ \to \mathbb{Q}^+$ is a group homomorphism, then $f(x) = cx$ for some constant c.

   Any $x, y \in \mathbb{Q}$ can each be expressed as a fraction of integers, and in particular we can express them as fractions with a common denominator, $x = a/n$ and $y = b/n$. Let $c = nf(1/n)$, so that $f(1/n) = c/n$. If $a \geq 0$ then

   $$f(x) = f(\underbrace{1/n + \cdots + 1/n}_{a \text{ times}}) = \underbrace{f(1/n) + \cdots + f(1/n)}_{a \text{ times}} = ac/n = cx$$

   and if $a < 0$ then

   $$f(x) = f(\underbrace{-1/n - \cdots - 1/n}_{-a \text{ times}}) = \underbrace{-f(1/n) - \cdots - f(1/n)}_{-a \text{ times}} = ac/n = cx.$$

   By the same argument, $f(y) = cy$. Since every pair of inputs is scaled by the same constant, it must be that $f(x) = cx$ for all $x \in \mathbb{Q}$.

   (b) Let V and W be vector spaces over $\mathbb{Q}$ and $T : V \to W$ a function. Prove that T is a group homomorphism between $(V, +)$ and $(W, +)$ if and only if T is a linear map.

   If $T : V \to W$ is a linear map then it satisifies $T(x+y) = T(x)+T(y)$ for all $x, y \in V$ and $T(kx) = kT(x)$ for all $k \in \mathbb{Q}$ and $x \in V$. The first property implies that T is a group homororomphism from $(V, +)$ to $(W, +)$.

   If $T : V \to W$ is a homomorphism between the additive groups, then $T(x + y) = T(x) + T(y)$ for all $x, y \in V$. Let $k \in \mathbb{Q}$ and $x \in V$, so $k = a/b$ for some integers a, b with $b > 0$. Let $z = (1/b)x$ so $x = bz$ and $kx = az$. Then if $b \geq 0$,

   $$T(x) = T(\underbrace{z + \cdots + z}_{b \text{ times}}) = bT(z)$$

or if $b < 0$,

$$T(x) = T(\underbrace{-z - \cdots - z}_{-b \text{ times}}) = -bT(-z) = bT(z).$$

Similarly

$$T(kx) = T(\underbrace{z + \cdots + z}_{a \text{ times}}) = aT(z).$$

Therefore $T(kx) = (a/b)T(x) = kT(x)$. This proves that T is a linear map.

(c) Is the property in part (a) true for $f : \mathbb{C}^+ \to \mathbb{C}^+$?

No. Consider the map $f(z) = \mathrm{Re}(z)$ that outputs the real part of a complex number z. This is an additive group homomorphism since $\mathrm{Re}(z + w) = \mathrm{Re}(z) + \mathrm{Re}(w)$. However $\mathrm{Re}(1) = 1 \cdot 1$ while $\mathrm{Re}(i) = 0 \cdot i$ so 1 and i are not scaled by the same value.

(d) Is the property in part (a) true for $f : \mathbb{R}^+ \to \mathbb{R}^+$?

No. $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield, so $\mathbb{R}$ is a vector space over $\mathbb{Q}$. Every vector space has a basis, so there exists a basis B for $\mathbb{R}$ as a $\mathbb{Q}$-vector space (although constructing such a basis concretely is essentially impossible). As a counterexample to the property in (a), consider $\mathbb{Q}$-linear map $f : \mathbb{R} \to \mathbb{R}$ that scales the different basis elements of B by different amounts. Since the map is linear, it satisfies the property that $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$, so f is an additive group homomorphism, but it doesn't scale all the elements of $\mathbb{R}$ by the same amount.