1. Show that the following rules constitute (left) group actions on the specified sets:

(a) Let F be a field and $F^{\times} = F\backslash\{0\}$ the multiplicative group of nonzero elements of F. Then $F^{\times}$ acts on F via $g \cdot a = ga$ where $g \in F^{\times}, a \in F$.

i: Let $a \in A, g_1, g_2 \in F^{\times}$. Then

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a) &= g_1(g_2 a) \\ &= (g_1 g_2)a \qquad \text{(associativity of multiplication over } F\text{)} \\ &= (g_1 g_2) \cdot a \qquad (F^{\times} \text{ closed under multiplication}) \end{aligned}$$

ii: $1 \cdot a = 1a = a$ since 1 is the identity in both groups.

Therefore, it is a group operation.

(b)The additive group $\mathbb{R}$ acts on $\mathbb{R}^2$ via $r \cdot (x, y) = (x + ry, r)$. Note that $\mathbb{R}$ is a field so we have distributivity, associativity of addition, and commutativity of addition.

i: Let $r_1, r_2 \in \mathbb{R}$ and let $(x, y) \in \mathbb{R}^2$. Then

$$\begin{aligned} r_1 \cdot (r_2 \cdot (x, y)) = r_1 \cdot (x + r_2 y, y) &= ((x + r_2 y) + r_1 y, y) \\ = (x + (r_2 y + r_1 y, y)) &= (x + (r_2 + r_1)y, y) \\ = (x + (r_1 + r_2)y, y) &= (r_1 + r_2) \cdot (x, y) \end{aligned}$$

ii: 0 is the additive identity and $0 \cdot (x, y) = (x + 0y, y) = (x, y)$

Therefore, it is a group operation.

(c) Included on additional page.

1c) Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in GL_2(\mathbb{R})$ and $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$.

i) Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a'x + b'y \\ c'x + d'y \end{pmatrix}$

$$= \begin{pmatrix} aa'x + ab'y + bc'x + bd'y \\ ca'x + cb'y + dc'x + dd'y \end{pmatrix}$$

$$= \begin{pmatrix} (aa' + bc')x + (ab' + bd')y \\ (ca' + dc')x + (cb' + dd')y \end{pmatrix}$$

$$= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

$$= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$ ✓ ✓

(ii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1x + 0y \\ 0 + 1y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$. And $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is a 2×2 invertible matrix. ✓

Therefore, it satisfies the definition of a (left) group action.

2. Let $\varphi : G \to S_A$ be the permutation reputation associated with $G \circlearrowleft A$. By definition $\ker G \circlearrowleft A = \{g \in G : g \cdot a = a \forall a \in A\}$. Also

$$\begin{aligned}\ker \varphi &= \{g \in G : \varphi(g) = 1\} \\ &= \{g \in G : \varphi(g)(a) = 1(a) \forall a \in A\} \\ &= \{g \in G : g \cdot a = a \ \forall a \in A\} \\ &= \ker G \circlearrowleft A\end{aligned}$$

Therefore, the kernel of an action of the group G on a set A is the same as the corresponding permutation representation.

4. Let G be an abelian group and $X = \{g \in G : |g| < \infty$.

i: $|1| = 1$ for all groups. Therefore, $X \neq \varnothing$.

ii: Let $a, b \in X$. Then $|a| = n_a < \infty$ and $|b| = n_b < \infty$¿. Let $n = lcm(n_a, n_b)$. Then there exist some $k_a, k_b \in \mathbb{Z}^+$ such that $k_a n_a = n$ and $k_b n_b = n$. Thus,

$$\begin{aligned}(ab)^n &= a^n b^n && \text{(since } G \text{ is abelian)}\\ &= a^{k_a n_a} b^{k_b n_b} = (a^{n_a})^{k_a}(a^{n_b})^{k_b}\\ &= 1^{k_a} 1^{k_b} = 1\end{aligned}$$

Therefore, $|ab| \leqslant n < \infty$. Thus, X is closed under multiplication.

iii: Let $a \in X$. Then $|a| = n < \infty$. I claim $|a^{-1}| \leqslant n < \infty$. Since $a^n = 1$, $a^{-1} = a^{n-1}$. Thus

$$(a^{-1})^n = (a^{n-1})^n = (a^n)^{n-1} = 1^{n-1} = 1$$

Therefore, a^{-1} has finite order.

Thus, the torsion subgroup, X, is a subgroup.

Matrix example from class attached at end. Why?

P4: Example: Let $A=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ and $B=\begin{pmatrix}0&2\\\frac{1}{2}&0\end{pmatrix}$. Then $AA=I$ and $BB=I$, so $A,B\in GL_2(\mathbb{R})$ and $|A|=|B|=2$. However,

$$AB=\begin{pmatrix}\frac{1}{2}&0\\0&2\end{pmatrix}$$

Therefore, $(AB)^n=\begin{pmatrix}(\frac{1}{2})^n&0\\0&2^n\end{pmatrix}\neq\begin{pmatrix}1&0\\0&1\end{pmatrix}$ for all $n\in\mathbb{Z}^+$. Thus $|AB|=\infty$. So $\{g\in GL_2(F): |g|<\infty\}$ is not a subgroup

yes, good job

5. Since all elements of $\mathbb{Z}$ have infinite order except for 0, $\tau_{\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}} = \{(0,b) | b \in \mathbb{Z}/n\mathbb{Z}\}$. Since both $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are abelian their direct product will be abelian as well. As was shown in problem 4, if G is abelian, then τ_G is a subgroup. ✓

$\mathbb{Z} \times /n\mathbb{Z} - (\tau_{\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}}) \cup \{(0,0)\}$, the union of the set of all infinitely ordered elements with the identity element cannot be a subgroup as it cannot be closed under products. Suppose (x, y) is not the identity element and has infinite order. $x \in \mathbb{Z}$, so $\exists x^{-1} \in \mathbb{Z}$. (x^{-1}, y) will also have infinite order because no matter how many times you subtract x from $-x$, it will never cycle back to 0. However $(x,y)(-x,y) = (0,y)$, so long as $y \in \mathbb{Z}/n\mathbb{Z}$ is not 0. $(0,y) \in \tau_{\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}}$ and is not the identity element. This means that the product of two elements in the set of infinite order elements does not necessarily have infinite order itself. Thus the set cannot constitute a subgroup, by definition. good

possibly problematic way to think about stuff

Problem 6:

Prove if $H, K \leq G$, then $H \cap K \leq G$.

Bonus: Prove if A is a collection of subgroups of G, $\bigcap_{H \in A} H \leq G$.

I will prove the bonus. ✓

Since both proofs are similar,

Let $J = \bigcap_{H \in A} H$. Since each $H \leq G$, each H contains I.

So $I \in J$. Let $a, b \in J$. Then $a, b \in H$ for all $H \in A$ and

since each H is a subgroup of G, $ab^{-1} \in H$ for all H.

So, $ab^{-1} \in J$. ✓ Hence by the subgroup criterion, $J \leq G$.

5

great job.

7. Let $A \leq GL_2(F_3)$ ~~[scribbled out]~~ be generated by $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ & $b = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Note that $a^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$ ✓

and $b^4 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 2^2 & 0 \\ 0 & 2^2 \end{pmatrix} = I$ ($2^2 = 1$ in F_3).

Thus, $|a| = |b| = 4$. Furthermore; $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = -\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$\Rightarrow ab = -ba$. Q_8 we know is generated by i, j where $ij = -ji$ and $i^4 = j^4 = 1$.

So let φ be the homomorphism taking $Q_8 \to A$. φ is surjective since it just takes the generators i, j of Q_8 to the generators a, b of A. Finally, since

OK.

$|A| = 8 = |Q_8|$, ✓ φ is also an isomorphism $\Rightarrow$ $A \cong Q_8$ ✓ $\square$

Problem 8. A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.

(a) Prove that every finite group is finitely generated.
$\langle H \rangle$ is a finite set that generates H (there may be smaller ones, but that is sufficient). ✓

(b) Prove that $\mathbb{Z}$ is finitely generated.
$\langle 1 \rangle$ generates $\mathbb{Z}$ because $1^n = n \forall n \in \mathbb{Z}$ (including negative powers). -1 is also acceptable as a generating element. ✓

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leqslant \langle 1/k \rangle$ where k is the product of all the denominators which appear in a set of generators for H.]
If H is generated by $\langle a_1, a_2, a_3, \cdots, a_m \rangle$ where $a_i = \frac{p_i}{q_i}$ expressed in simplest form, then elements of H can be expressed as $\sum_{i=1}^{m} n_i a_i$ and as

such H contains all fractions obtainable by summing the fractions indexed. All of these fractions will be of the form $\frac{c}{\prod_{i=1}^{m} q_i}$, that is they will be expressible in terms of the least common denominator $(a_1, a_2, \cdots, a_n)$. Thus $H \leqslant \langle 1/k \rangle$ and in fact $H = \langle \frac{1}{(a_1, a_2, \cdots, a_n)} \rangle$ and so H is cyclic. Wow.

(d) Prove that $\mathbb{Q}$ is not finitely generated.

Note that $\mathbb{Q}$ contains fractions with any integer as their denominator in simplest form. In particular, $\mathbb{Q}$ contains all fractions $1/p$ where p is a prime. There are an infinite number of primes, and because the LCD cannot introduce a prime factor not included in other denominators, $\mathbb{Q}$'s minimal generating set is $\langle 1/p \rangle$, which contains an infinite number of elements. So $\mathbb{Q}$ is not finitely generated. ✓

9. Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H.

(a) Clearly $\varphi^{-1}(E) \subseteq G$. Therefore, we only need to show it follows the subgroup criterion.

i: $1 \in E$ since E is a subgroup and $\varphi(1) = 1$ since φ is a homomorphism. Therefore, $1 \in \varphi^{-1}(E) \neq \emptyset$.

ii: Let $x, y \in \varphi^{-1}(E)$. Then there exists $a, b \in E$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Since E is a subgroup and φ is a homomorphism, $(\varphi(y))^{-1} = b^{-1} \in E$. Therefore,

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = ab^{-1} \in E$$

10. Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a+bi) = a^2 + b^2$. Let $(a+bi), (c+di) \in \mathbb{C}^\times$. Then

$$\begin{aligned}\varphi((a+bi)(c+di)) &= \varphi(ac + adi + bci - bd) = \varphi((ac-bd) + (ad+bc)i) \\ &= (ac-bd)^2 + (ad+bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= (a^2+b^2)(c^2+d^2) = \varphi(a+bi)\varphi(c+di)\end{aligned}$$

Therefore, φ is a homomorphism. The image of φ is $(\mathbb{R}^\times)^+$, i.e. the positive portion of the real multiplicative group.

The kernel of φ is the circle of radius one in the complex plane. More generally, the fibers of φ are the subsets of the complex that that lie on the circle of radius $\sqrt{a^2+b^2}$.